TEXTOS guíaUN

Teoría de grupos

Sebastián Castañeda Hernández
Ismael Gutiérrez García
y Jorge Robinson Evilla

EDITORIAL uninorte

TEORÍA DE GRUPOS

Sebastián Castañeda Hernández
Ismael Gutiérrez García
Jorge Robinson Evilla

EDITORIAL
uninorte

Castañeda Hernández, Sebastián.
Teoría de grupos / Sebastián Castañeda Hernández, Ismael Gutiérrez García, Jorge Robinson Evilla. -- Barranquilla, Colombia: Editorial Universidad del Norte, 2022.

239 páginas : ilustraciones ; 28 cm.
Incluye índice alfabético (páginas 237-240)
ISBN 978-958-789-347-2 (PDF)

1. Teoría de los grupos -- Problemas, ejercicios, etc. I. Gutiérrez García, Ismael. II. Robinson Evilla, Jorge. III. Tit.

(512.22 C346) (CO-BrUNB)

UNIVERSIDAD DEL NORTE
Vigilada Mineducación
www.uninorte.edu.co
Km 5, vía a Puerto Colombia, A.A. 1569
Área metropolitana de Barranquilla (Colombia)

© Universidad del Norte, 2022
Sebastián Castañeda Hernández, Ismael Gutiérrez García y Jorge Robinson Evilla

Coordinación editorial
María Margarita Mendoza

Asistencia editorial
Fabián Buelvas

Diagramación
Ismael Gutiérrez García

Corrección de textos
Henry Stein

Diseño de portada
Silvana Pacheco

Revisión y arte final
Munir Kharfan

Hecho en Colombia
Made in Colombia

© Reservados todos los derechos. Queda prohibida la reproducción total o parcial de esta obra por cualquier medio reprográfico, fónico o informático, así como su transmisión por cualquier medio mecánico o electrónico, fotocopias, microfilm, *offset*, mimeográfico u otros sin autorización previa y escrita de los titulares del *copyright*. La violación de dichos derechos constituye un delito contra la propiedad intelectual.

A Elena y Matthias

ÍNDICE GENERAL

Prólogo **13**

Lista de tablas **13**

Lista de figuras **13**

1 Preliminares **15**

1.1 Primeras definiciones y ejemplos 16

1.2 Subgrupos 22

1.3 Clases laterales y transversales 35

1.4 Grupos finitos hasta orden 5 40

1.5 Ejercicios 42

2 Homomorfismos de grupos **47**

2.1 Subgrupos normales y grupo cociente 48

2.2 Homomorfismos 52

2.3 Endomorfismos y automorfismos 61

2.4 Conjugación 64
2.5 Ejercicios 70

3 Grupo simétrico y grupo alternante **77**
3.1 La notación de ciclos 77
3.2 El signo de una permutación 80
3.3 El grupo alternante 83
3.4 Ejercicios 87

4 Grupos cíclicos **89**
4.1 Elementos de torsión 89
4.2 Subgrupos de grupos cíclicos 95
4.3 Clasificación de los grupos cíclicos 98
4.4 El grupo de automorfismos de un grupo cíclico 100
4.5 Ejercicios 103

5 Productos directos y semidirectos **105**
5.1 Producto directo externo - caso finito 105
5.2 Producto directo interno 110
5.3 Producto directo externo - caso infinito 115
5.4 Suma directa externa - caso infinito 118
5.5 Producto semidirecto 124
5.6 Ejercicios 128

6 Los teoremas de Sylow **131**
6.1 Representaciones por permutaciones y G-conjuntos 131
6.2 Los p-subgrupos de Sylow 140

6.3 Algunas aplicaciones 148
6.4 Grupos abelianos finitos y finitamente generados 151
6.5 Ejercicios 155

7 Grupos solubles **159**

7.1 Conmutadores y el subgrupo derivado 159
7.2 Derivados de orden superior 166
7.3 Grupos solubles finitos 168
7.4 Ejercicios 171

8 Grupos nilpotentes **173**

8.1 Series centrales 173
8.1.1 Serie central descendente 174
8.1.2 Serie central ascendente 176
8.2 Grupos nilpotentes finitos 178
8.3 Nilpotencia implica solubilidad 183
8.4 Ejercicios 185

9 El teorema de Jordan-Hölder **189**

9.1 El lema de Zassenhaus 189
9.2 El teorema de Schreier 193
9.3 El teorema de Jordan-Hölder 196
9.4 Series de composición y grupos solubles 198
9.5 Subgrupos normales minimales 199

10 Nilpotencia y solubilidad - Parte 2 **203**

10.1 El subgrupo de Frattini 203

10.2 El subgrupo de Fitting 210

11 Algunos Teoremas de P. Hall **215**

11.1 El teorema de Schur-Zassenhaus 216

11.2 Los π-subgrupos de Hall 222

11.3 Ejercicios 228

LISTA DE FIGURAS

1.1 Isometrías de un rectángulo 18

1.2 n-esimas raíces complejas de la unidad para $n = 5$ 24

1.3 Generadores del grupo dihédrico de grado n 27

1.4 Raíces 3-ésimas o cúbicas de la unidad 28

1.5 Simetrías del triángulo 28

1.6 Simetrías del cuadrado 29

2.1 El grupo cociente 50

5.1 Producto semidirecto interno 127

9.1 Lema de Zassenhaus 191

9.2 Refinamiento 194

LISTA DE TABLAS

1.1 Tabla de multiplicación del 4-grupo de Klein 18
1.2 Tabla de multiplicación del grupo D_8 30
1.3 Tabla de multiplicación del grupo de los cuaterniones 32

5.1 Tabla de multiplicación del grupo $\mathbb{Z}_2 \times \mathbb{Z}_2$ 106
5.2 Tabla de multiplicación del grupo $\mathbb{Z}_5 \times \mathbb{Z}_2$ 106
5.3 Tabla de multiplicación del grupo $\mathbb{Z}_4 \rtimes_\alpha \mathbb{Z}_2$ 126

6.1 Grupos abelianos de orden 1000 153
6.2 Clasificación de los grupos hasta orden 15 154

PRÓLOGO

Iniciamos los comentarios sobre este libro destacando la importancia de la teoría de grupos como componente de la estructura del álgebra y de las matemáticas modernas en general. Los principales objetivos de este texto son: despertar el interés de los estudiantes en tan útiles e interesantes temáticas, presentar contenidos que estén al alcance de nuestros estudiantes de pregrado y al tiempo facilitar la comprensión con claras explicaciones y abundantes ejemplos.

Iniciamos nuestro desarrollo teórico con preliminares que incluyen el teorema de Lagrange y los grupos finitos hasta orden 5. Después se analizan los homomorfismos de grupos, el grupo simétrico y los grupos cíclicos. Luego, para facilitar el estudio de los teoremas de Sylow, se presentan los productos directos y semidirectos y la acción de un grupo sobre un conjunto. El libro termina abordando los grupos solubles, los nilpotentes, el teorema de Jorden-Hölder y los clásicos teoremas de P. Hall.

Aunque los conocimientos de teoría de grupos que aparecen en este libro son conocidos, creemos que el modo de presentarlos facilita su lectura y comprensión, pues ha sido nuestro deseo presentar los temas a modo de simplificación de la teoría que aparece en los libros ya tradicionales de grupos. No significa esto que se ha descuidado la formalización, sino que nuestros esfuerzos se han concentrado en explicar y relacionar las ideas y argumentos de forma tal que el estudiante pueda acceder a ellos sin mayores dificultades.

Les invitamos, pues, a disfrutar y crecer con esta lectura, así como nosotros lo hicimos con la elaboración del texto.

CAPÍTULO 1

PRELIMINARES

Dinero, maquinización, álgebra.
Los tres monstruos de la civilización actual.
Analogía perfecta.
(Simone Weil)

Durante el siglo XVIII, la teoría de grupos consistía en el estudio grupos finitos de permutaciones y grupos de transformaciones geométricas. Algunos trabajos importantes en esta dirección se deben a F. Klein[1]. No obstante, durante todo el siglo XIX se presentaron desarrollos significativos en la teoría. La forma abstracta del concepto de grupo se remonta a 1854 con los trabajos de A. Cayley[2] para grupos finitos, a 1870 con L. Kronecker[3] para grupos abelianos y en forma definitiva a 1892 con H. Weber[4].

La evolución de la teoría de grupos estuvo influenciada por diversos factores propios del pensamiento de ese siglo. Entre otras podemos destacar la aparición del razonamiento abstracto, una preocupación por el rigor matemático y la visión de las matemáticas como una actividad humana admisible independiente del mundo físico.

[1]Felix Christian Klein (Düsseldorf, 1849-Göttingen, 1945), matemático alemán. Presentó una excelente clasificación de la geometría.

[2]Arthur Cayley (Reino Unido, 1821-Cambridge, 1895), matemático británico. Es el tercer matemático más prolífico de la historia, sobrepasado solo por Euler y Cauchy.

[3]Leopold Kronecker (Liegnitz, 1823-Berlín, 1891), matemático alemán. Estuvo en contra de varias de las extensiones matemáticas de G. Cantor.

[4]Heinrich Weber (Heidelberg, 1842-Strasburg, 1913), matemático alemán. Formuló de manera abstracta la teoría de Galois.

1.1 Primeras definiciones y ejemplos

Introducimos en esta sección algunos resultados que son consecuencias inmediatas de las definición de grupo.

1.1.1 Definición. Sea G un conjunto no vacío. Una `operación binaria` f sobre G es una función $f : G \times G \longrightarrow G$. Usualmente, en lugar de $f(x, y)$ escribimos xy, $x \cdot y$, $x * y$, $x \circ y$, $x + y$, entre otras.

1.1.2 Definición. Sea $(x, y) \longmapsto x \cdot y$ una operación binaria definida sobre un conjunto no vacío G. Decimos que la pareja $(G, \cdot)$ es un `grupo` si se verifican los siguientes axiomas:

(G1) `Asociatividad`. Para todo $x, y, z \in G$

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z.$$

(G2) `Existencia de un elemento neutro o identidad`. Existe $e \in G$ tal que para todo $x \in G$

$$e \cdot x = x \cdot e = x.$$

(G3) `Existencia de inversos`. Para todo $x \in G$ existe $y \in G$ tal que

$$x \cdot y = y \cdot x = e.$$

Si además se verifica que $x \cdot y = y \cdot x$ para todo $x, y \in G$, entonces decimos que G es un grupo `abeliano` o `conmutativo`. Si G es un conjunto finito, entonces el número de elementos de G lo llamamos `orden` de G y lo notamos con $|G|$.

1.1.3 Ejemplos. (1) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Q}^\times, \cdot)$, $(\mathbb{R}^\times, \cdot)$ y $(\mathbb{C}^\times, \cdot)$ son grupos.

(2) Sea $K[x]$ el conjunto de los polinomios con coeficientes en un cuerpo K. Entonces $(K[x], +)$ es un grupo.

(3) Si R es alguno de los anillos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$, entonces el conjunto de las matrices de tamaño $n \times n$ con entradas en R, notado con $\mathbf{M}_n(R)$, es un grupo abeliano con la suma usual de matrices.

(4) Sea $\mathrm{GL}_n(K) = \{A \mid A \in \mathrm{Mat}(n, K),\ \det(A) \neq 0\}$. Entonces $\mathrm{GL}_n(K)$ es un grupo con respecto a la multiplicación usual de matrices y lo llamamos `grupo lineal general` de grado n sobre K.

Si K es el cuerpo finito con p elementos, el cual notamos con $\mathbb{F}_p$, siendo p un número primo, entonces escribimos $\mathrm{GL}_n(p)$ en lugar de $\mathrm{GL}_n(\mathbb{F}_p)$. Por ejemplo, si $n = p = 2$, entonces

$$\mathrm{GL}_2(2) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}.$$

Note que

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \text{ y } \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Por lo tanto, $\mathrm{GL}_2(2)$ es un grupo no abeliano de orden 6.

(5) Sea $\mathrm{SL}_n(K) = \{A \mid A \in \mathrm{GL}_n(K),\ \det(A) = 1\}$. Entonces $\mathrm{SL}_n(K)$ es un grupo con respecto a la multiplicación usual de matrices y se denomina `grupo lineal especial` de grado n sobre K.

1.1.4 Ejemplo. (El grupo simétrico de grado n) Dado un conjunto no vacío X, una función biyectiva $\sigma : X \longrightarrow X$ se denominará una permutación de X. El conjunto de tales biyecciones, notado con $\mathrm{Sym}(X)$, es un grupo con respecto de la composición de funciones. Este grupo se denomina `grupo de permutaciones` de X. Una representación usual para una permutación $\sigma \in \mathrm{Sym}(X)$ es la siguiente:

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix} \tag{1.1}$$

Si $X = \{1, \ldots, n\}$, entonces escribimos $\mathrm{Sym}(n)$ y hablamos del `grupo simétrico de grado` n. Por ejemplo, si $X = \{1, 2, 3\}$, entonces los elementos de $\mathrm{Sym}(3)$ son:

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Sea $k \in \mathbb{N}$. Una permutación $\sigma \in \mathrm{Sym}(n)$ se denomina un k-ciclo si existe un conjunto $A = \{a_1, \ldots, a_k\} \subseteq X$ tal que $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3$, …, $\sigma(a_{k-1}) = a_k$, $\sigma(a_k) = a_1$ y $\sigma(x) = x$ para todo $x \in \Omega \setminus A$. Para abreviar utilizamos la notación

$$\sigma = (a_1\ a_2 \ldots a_k).$$

Note que los k-ciclos $(a_1\ a_2 \ldots a_k)$ y $(a_k\ a_1 \ldots a_{k-1})$ representan la misma permutación.

Usando la notación de k-ciclos y asumiendo que la función identidad se representa con (1) se tiene que

$$\mathrm{Sym}(3) = \{(1), (23), (13), (12), (123), (132)\}.$$

Para $n \geq 3$ se verifica que $\mathrm{Sym}(n)$ no es abeliano.

1.1.5 Ejemplo. (El grupo de isometrías de un rectángulo o 4-grupo de Klein) Una transformación isométrica, o simplemente una isometría, de un rectángulo es un movimiento que deja fija la figura. Es decir, con el movimiento no se alteran ni la forma ni el tamaño del rectángulo.

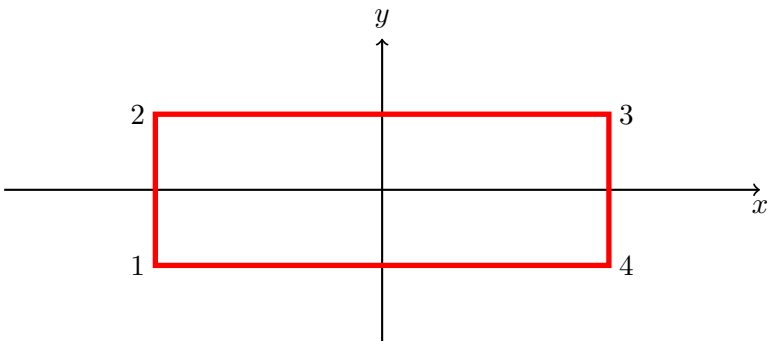


Figura 1.1: Isometrías de un rectángulo

Las isometrías que fijan el rectángulo son:

- La identidad: (1)
- La simetría con respecto al eje x: $g = (12)(34)$
- La simetría con respecto al eje y: $h = (14)(23)$
- La simetría con respecto al centro: $k = (13)(24)$

La composición de dos isometrías que fijan el rectángulo es una isometría que fija el rectángulo. Entonces el conjunto $G = \{1, g, h, k\}$ y la composición es un grupo. Este grupo es usualmente llamado `4-grupo de Klein` y se nota con V_4. Su tabla de multiplicación se muestra a continuación:

$\cdot$	(1)	g	h	k
(1)	(1)	g	h	k
g	g	(1)	k	h
h	h	k	(1)	g
k	k	h	g	(1)

Tabla 1.1: Tabla de multiplicación del 4-grupo de Klein

1.1.6 Lema. Sea G un grupo. Entonces

(1) Existe un único $e \in G$ con $e \cdot x = x \cdot e = x$ para todo $x \in G$.

(2) Para todo $x \in G$ existe un único $y \in G$ tal que $y \cdot x = x \cdot y = e$. Llamaremos a y el `inverso` de x y lo notaremos con x^{-1}. Si G es abeliano, entonces este se escribe aditivamente y notamos el inverso de x con $-x$.

DEMOSTRACIÓN. (1) Note que $e = e \cdot e' = e'$.

(2) Sean y y z inversos de $x \in G$. Entonces

$$z = e \cdot z = (y \cdot x) \cdot z = y \cdot (x \cdot z) = y \cdot e = y,$$

con lo cual se tiene la afirmación. □

1.1.7 Observaciones. (1) No escribiremos a lo largo del texto el símbolo $\cdot$ para denotar una operación binaria. A partir de ahora usamos la yuxtaposición y la llamamos `producto` o `multiplicación`. Es decir, en lugar de $x \cdot y$ escribimos implemente xy. Además, en lugar de $(G, \cdot)$ escribimos simplemente G.

(2) En lo que sigue el elemento identidad de un grupo G es denotado con 1, y si el grupo es abeliano, entonces usamos 0 para representar el elemento identidad de G.

1.1.8 Lema. Sea G un grupo y $x, y \in G$. Entonces

(1) $(x^{-1})^{-1} = x$,

(2) $(xy)^{-1} = y^{-1}x^{-1}$.

DEMOSTRACIÓN. (1) Dado que $xx^{-1} = 1 = x^{-1}x$, se tiene que x es el inverso de x^{-1}.

(2) Usando la asociatividad se sigue que

$$(y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}x)y = y^{-1}(1y) = y^{-1}y = 1.$$

Similar se demuestra que $(xy)(y^{-1}x^{-1}) = 1$. □

1.1.9 Lema. (Leyes de cancelación) Sea G un grupo, $a, x, y \in G$. Entonces

(1) Si $ax = ay$, entonces $x = y$

(2) Si $xa = ya$, entonces $x = y$.

Demostración. Note que

$$x = 1x = (a^{-1}a)x = a^{-1}(ax) = a^{-1}(ay) = (a^{-1}a)y = 1y = y.$$

Similarmente se demuestra la otra afirmación. □

1.1.10 Definición. Sea G un grupo, $g \in G$ y $n \in \mathbb{Z}$. Definimos recursivamente la n-ésima potencia de g, notada en caso multiplicativo con g^n o en caso aditivo con ng de la siguiente manera:

$$g^n := \begin{cases} 1 & \text{si } n = 0 \\ g^{n-1}g, & \text{si } n > 0 \\ (g^{-n})^{-1}, & \text{si } n < 0. \end{cases}$$

En el caso abeliano se tiene que

$$ng := \begin{cases} 0, & \text{si } n = 0 \\ (n-1)g + g, & \text{si } n > 0 \\ -((-n)g), & \text{si } n < 0 \end{cases}$$

1.1.11 Teorema. Sea G un grupo y $g \in G$. Para $n, m \in \mathbb{Z}$ se cumple:

(1) $g^m g^n = g^{m+n} = g^n g^m$.

(1) $mg + ng = (m+n)g = ng + mg$ (notación aditiva).

(2) $(g^m)^n = g^{mn}$.

(2) $n(mg) = (mn)g$ (notación aditiva).

Demostración. (1) Supongamos inicialmente que $m, n \in \mathbb{N}_0$ y demostramos la afirmación por inducción sobre n.

Paso 1. Si $n = 0$, entonces $g^m g^0 = g^m 1 = g^m = g^{m+0}$.

Hipótesis inductiva. Sea $n > 0$ y supongamos que la afirmación es válida para $n - 1$. Entonces

$$g^m g^n = g^m(g^{n-1}g) = (g^m g^{n-1})g = g^{m+n-1}g = g^{m+n}. \tag{1.2}$$

Demostramos la siguiente afirmación: Si g es invertible y $k \in \mathbb{N}$, entonces $g^{-k}g = g^{-k+1}$. Dado que $k - 1 \geq 0$ de (1.2), se sigue que $gg^{k-1} = g^k$. Entonces

$$g^{-k} = (g^k)^{-1} = (gg^{k-1})^{-1} = g^{-(k-1)}g^{-1} = g^{-k+1}g^{-1}.$$

Multiplicando por g a ambos lados de la igualdad se tiene que

$$g^{-k}g = (g^{-k+1}g^{-1})g = g^{-k+1}. \tag{1.3}$$

De la definición de potencia y de (1.3) se sigue que $g^{m+n}g = g^{m+n+1}$ para todo $m, n \in \mathbb{Z}$. En efecto, si $m + n \geq 0$, la afirmación se sigue de la definición de potencia, y si $m + n < 0$, entonces esta se sigue de (1.3).

Similar como antes se puede demostrar, por inducción sobre n, que $g^m g^n = g^{m+n}$ para todo $m \in \mathbb{Z}$ y para todo $n \in \mathbb{N}_0$. Si demostramos que para $m \in \mathbb{Z}$ y $n > 0$ se verifica que $g^m g^{-n} = g^{m-n}$, entonces se tiene completa la demostración de (1).

Note que $g^{m-n}g^n = g^{m-n+n} = g^m$. Entonces si multiplicamos a ambos lados por $(g^n)^{-1}$ se tiene que $g^{m-n} = g^m(g^n)^{-1} = g^m g^{-n}$.

(2) De la definición de potencia se tiene que $g^{-m} = (g^m)^{-1}$ para todo $m \geq 0$. Si $m < 0$, entonces $(g^m)^{-1} = ((g^{-m})^{-1})^{-1} = g^{-m}$. Por lo tanto, $(g^m)^{-1} = g^{-m}$ para todo $m \in \mathbb{Z}$.

Demostramos por inducción sobre n que: $(g^m)^n = g^{mn}$ para todo $m \in \mathbb{Z}$ y $n \in \mathbb{N}_0$.

Paso 1. Si $n = 0$, entonces $(g^m)^0 = 1 = g^0 = g^{m0}$.

Hipótesis inductiva. Supongamos que la afirmación es válida para $n \geq 0$. Entonces

$$(g^m)^{n+1} = (g^m)^n g^m = g^{mn}g^m = g^{mn+m} = g^{m(n+1)}.$$

Sea ahora $n \geq 0$ y g es invertible. Entonces

$$(g^m)^{-n} = ((g^m)^n)^{-1} = (g^{mn})^{-1} = g^{-mn}. \quad \square$$

1.1.12 Definición. Sea G un grupo y $g \in G$. El `orden` de g se define como el número natural más pequeño n si existe tal que $g^n = 1$. Si tal número existe, lo notamos con $\text{ord}(g)$, en caso contrario decimos que g tiene orden infinito.

1.1.13 Ejemplos. (1) Si G es un grupo finito, entonces todos sus elementos tienen orden finito.

(2) Sea $G = \text{Sym}(3)$. Entonces, $\text{ord}((12)) = 2$.

(3) Para todo $0 \neq g \in \mathbb{Z}$ se verifica que $\text{ord}(g) = \infty$.

(4) En V_4 se verifica que todos sus elementos distintos de 1 tienen orden 2.

1.2 Subgrupos

Consideramos ahora subconjuntos de un grupo dado G, los cuales, al considerar la restricción de la operación de G sobre ellos, tienen la estructura de grupo.

1.2.1 Definición. Sea G un grupo y $\varnothing \neq U \subseteq G$. Decimos que U es un **subgrupo** de G, notado $U \leq G$, si al restringir la operación $\cdot$ al conjunto U se verifica que $(U, \cdot)$ es un grupo. Si U es un subgrupo de G y $U \neq G$, entonces decimos que U es un **subgrupo propio** de G y lo notaremos con $U < G$. Un subgrupo $U < G$ se llama **maximal** en G si de $U < V \leq G$ se sigue que $V = G$. En este caso escribiremos $U \lneq G$.

1.2.2 Ejemplos. (1) Si G es un grupo, entonces $\{1\}$ y G son subgrupos de G. Estos se denominan `subgrupos triviales` de G. En adelante usamos el símbolo 1 para denotar el subgrupo trivial $\{1\}$ de cualquier grupo.

(2) $\mathbb{Z} \leq \mathbb{Q}$, $\mathbb{Q} \leq \mathbb{R}$ y $\mathbb{R} \leq \mathbb{C}$ con respecto a la suma.

(3) $\mathbb{Q}^\times \leq \mathbb{R}^\times$ y $\mathbb{R}^\times \leq \mathbb{C}^\times$ con respecto a la multiplicación.

(4) $\mathrm{SL}_n(K) \leq \mathrm{GL}_n(K)$.

1.2.3 Teorema. (Un criterio para subgrupos) Sea G un grupo y $\varnothing \neq U \subseteq G$. Las siguientes afirmaciones son equivalentes:

(1) $U \leq G$.

(2) Para todo $x, y \in U$ se verifica que $xy \in U$ y $x^{-1} \in U$.

(3) Para todo $x, y \in U$ se verifica que $x^{-1}y \in U$.

(4) Para todo $x, y \in U$ se verifica que $xy^{-1} \in U$.

Demostración. (1) $\Rightarrow$ (2). Sean $x, y \in U$. Dado que U es un subgrupo de G, se verifica inmediatamente que $xy \in U$ y $x^{-1} \in U$.

(2) $\Rightarrow$ (3). Si $x, y \in U$, entonces por hipótesis $x, y^{-1} \in U$, y así $xy^{-1} \in U$.

(3) $\Rightarrow$ (4). Es claro que de (3) se sigue que $1 \in U$ y que para todo $x \in U$ se verifica que $x^{-1} \in U$. Por lo tanto, para todo $x, y \in U$ se tiene que $xy^{-1} = (x^{-1})^{-1}y^{-1} \in U$.

(4) $\Rightarrow$ (1). Sean $x, y \in U$. Entonces $1 = xx^{-1} \in U$. Con esto se tiene que, $x^{-1} = 1x^{-1} \in U$. Por lo tanto, $xy = x(y^{-1})^{-1} \in U$. La propiedad asociativa se verifica naturalmente para los elementos de U. $\square$

1.2.4 Ejemplo. (`Los subgrupos de los enteros`) Los subgrupos de $\mathbb{Z}$ son de la forma $n\mathbb{Z}$, con $n \in \mathbb{N}_0$ fijo. Si $U = \{0\}$, entonces $n = 0$. Supongamos entonces que $U \neq \{0\}$. Para todo $u \in U$ se verifica que $-u \in U$. Por lo tanto, a U pertenecen números naturales. El principio de buen orden nos garantiza que existe un número natural mínimo, digamos n, en U. Demostramos que $U = n\mathbb{Z}$.

Sea $u \in U$ cualquiera. Usando la división con resto se tiene que existen $q, r \in \mathbb{Z}$ tales que $u = nq + r$ con $0 \leq r < n$. Dado que $u, n \in U$, se tiene que $u - nq = r \in U$. En consecuencia, por la minimalidad de n se sigue que $r = 0$, y así $u = nq \in n\mathbb{Z}$. Esto demuestra que $U \subseteq n\mathbb{Z}$. La otra contenencia es inmediata.

1.2.5 Observación. Sean $m, n \in \mathbb{N}$. Note que $n\mathbb{Z} \subseteq m\mathbb{Z}$ si y solo si $m \mid n$. En consecuencia, los subgrupos maximales de $\mathbb{Z}$ son de la forma $p\mathbb{Z}$, con p un número primo.

En el siguiente lema demostramos que la intersección de una familia de subgrupos de un grupo G es también un subgrupo.

1.2.6 Lema. Sea $\{U_j\}_{j \in J}$ una familia de subgrupos de un grupo G. Entonces $\bigcap_{j \in J} U_j$ es un subgrupo de G.

Demostración. Definamos $D := \bigcap_{j \in J} U_j$. Dado que $1 \in U_j$ para todo $j \in J$, se tiene que $1 \in D$, es decir, D no es vacío. Sean ahora $u, v \in D$. Entonces $u, v \in U_j$ para todo $j \in J$. Por lo tanto, $uv \in U_j$ para todo $j \in J$, y así $uv \in D$, teniendo la afirmación. □

En el siguiente lema demostramos que la unión de subgrupos de un grupo G no necesariamente es un subgrupo de G.

1.2.7 Lema. Sean U y V subgrupos de un grupo G. Entonces $U \cup V \leq G$ si y solo si $U \subseteq V$ o $V \subseteq U$.

Demostración. Si $U \subseteq V$ o $V \subseteq U$, entonces es claro que $U \cup V \leq G$.

Recíprocamente, supongamos que $U \cup V \leq G$, pero $U \nsubseteq V$ y $V \nsubseteq U$. Sean $u \in U \setminus V$ y $v \in V \setminus U$. Entonces $uv \in U \cup V$. Sin perder generalidad, podemos suponer que $uv \in U$. Entonces $v \in U$, lo cual es una contradicción. □

1.2.8 Observación. $2\mathbb{Z}$ y $3\mathbb{Z}$ son subgrupos de $\mathbb{Z}$, no obstante $2\mathbb{Z} \cup 3\mathbb{Z} = \{0, \pm 2, \pm 3, \pm 4, \ldots\}$ no es un subgrupo de $\mathbb{Z}$. En efecto, $2 + 3 = 5 \notin (2\mathbb{Z} \cup 3\mathbb{Z})$.

El criterio anterior se simplifica para subgrupos finitos de un grupo.

1.2.9 Lema. (`Un criterio para subgrupos finitos`) Sea U un subconjunto finito de un grupo G. Si para todo $u, v \in U$ se verifica que $uv \in U$, entonces U es un subgrupo de G.

DEMOSTRACIÓN. Usando el lema 1.2.3, es suficiente demostrar que $u^{-1} \in U$ para todo $u \in U$. Si $u \in U$, entonces $\{u^n \mid n \in \mathbb{N}_0\} \subseteq U$. Dado que U es finito, se sigue que existen $i, j \in \mathbb{N}_0$ con $j > i$ tales que $u^i = u^j$. Es decir, $u^{j-i} = 1$, y se tiene $u^{j-i} = uu^{j-i-1} = 1$. En consecuencia, $u^{-1} = u^{j-i-1} \in U$. □

1.2.10 Observación. Observe que $\mathbb{N} \subseteq \mathbb{Z}$ y no es un subgrupo. Es decir, la condición de ser un conjunto finito es de gran importancia.

1.2.11 Ejemplo. (`Las` n`-ésimas raíces complejas de la unidad`) Sea $n \in \mathbb{N}$ y denotemos con $U(n)$ el conjunto de las n-esimas raíces complejas de la unidad. Esto es,

$$U(n) = \{z \in \mathbb{C} \mid z^n = 1\} = \{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}\},$$

donde $\zeta_n := e^{i2\pi/n}$. Dado que $1 \in U(n)$ para todo n, se tiene que $U(n)$ es no vacío y finito. Sean $a, b \in U(n)$. Entonces $(ab)^n = a^n b^n = 1$. Esto demuestra que $U(n)$ es cerrado bajo la multiplicación. Usando el lema anterior se tiene que $U(n) \leq \mathbb{C}^\times$.

Geométricamente podemos visualizar los elementos de $U(n)$ como los vértices de un polígono regular de n lados. En la figura 1.2 se ilustra el caso $n = 5$.

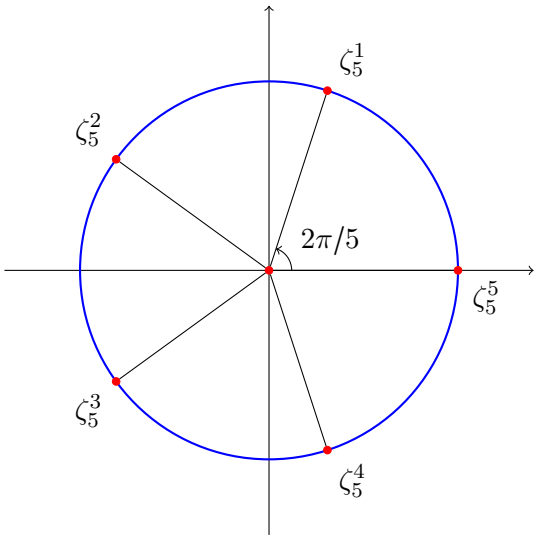


Figura 1.2: n-esimas raíces complejas de la unidad para $n = 5$

1.2.12 Ejemplo. En el ejemplo anterior vimos que para todo $n \in \mathbb{N}$ el conjunto $U(n)$ de

las n-ésimas raíces complejas de la unidad es un subgrupo de $\mathbb{C}^\times$. Si definimos ahora

$$G_\infty := \bigcup_{n\in\mathbb{N}} U(n),$$

entonces se tiene que G_∞ también es un subgrupo de $\mathbb{C}^\times$. Note que G_∞ es un grupo infinito en el que cada elemento tiene orden finito.

1.2.13 Definición. Sea G un grupo y $X \subseteq G$. La intersección de los subgrupos de G que contienen a X es denominada el subgrupo de G `generado` por X y se nota con $\langle X\rangle$. Si $G = \langle X\rangle$, entonces decimos que X genera a G y X es un `sistema de generadores` para G. Si X es finito, digamos $M = \{x_1, \ldots, x_k\}$, y genera a G, entonces G se dice `finitamente generado` y escribimos $G = \langle x_1, \ldots, x_k\rangle$ en lugar de $G = \langle\{x_1, \ldots, x_k\}\rangle$. Si $G = \langle g\rangle$ para algún $g \in G$, entonces G se llama `cíclico`.

Ahora demostramos que los elementos de $\langle X\rangle$ pueden verse como palabras que pueden formarse tomando como alfabeto al conjunto X.

1.2.14 Teorema. Sea G un grupo y $\varnothing \neq X \subseteq G$. Entonces

(1) $\langle X\rangle = \{x_1^{n_1}\cdots x_k^{n_k} \mid k \in \mathbb{N}, x_i \in X, n_i \in \mathbb{Z}\}$.

(1) $\langle X\rangle = \{n_1x_1 + \cdots + n_kx_k \mid k \in \mathbb{N}, x_i \in X, n_i \in \mathbb{Z}\}$ (En notación aditiva).

(2) Si $X = \{x_1, \ldots x_m\}$, un conjunto finito, y $x_ix_j = x_jx_i$ para $i \neq j$, entonces $\langle X\rangle$ es un grupo abeliano y $\langle X\rangle = \{x_1^{n_1}\cdots x_m^{n_m} \mid n_i \in \mathbb{Z}\}$.
En notación aditiva $\langle X\rangle = \{n_1x_1 + \cdots + n_mx_m \mid n_i \in \mathbb{Z}\}$.

(3) Si $X = \{x\}$, entonces $\langle X\rangle = \{x^n \mid n \in \mathbb{Z}\}$. En notación aditiva: $\langle X\rangle = \{nx \mid n \in \mathbb{Z}\}$.

(4) Si $X = \{x\}$ y $\operatorname{ord}(x)$ es finito, entonces $|\langle X\rangle| = \operatorname{ord}(x)$.

Demostración. (1) Sea U definido por $U := \{x_1^{n_1}\cdots x_k^{n_k} \mid k \in \mathbb{N},\ x_i \in X,\ n_i \in \mathbb{N}\}$. Demostramos que $U \leq G$ y $\langle X\rangle \subseteq U$. En efecto, si $x_i \in X$, entonces $x_i \in U$. Esto demuestra que $X \subseteq U$. Dado que $\varnothing \neq X \subseteq U$, se tiene que $U \neq \varnothing$. Sean $x = x_1^{n_1}\cdots x_k^{n_k}$ y $y = y_1^{n_1}\cdots y_s^{n_s}$ elementos de U. Entonces $xy = x_1^{n_1}\cdots x_k^{n_k}y_1^{n_1}\cdots y_s^{n_s} \in U$, con lo cual $U \leq G$ y, en consecuencia, $\langle X\rangle \subseteq U$.

Recíprocamente, sabemos que $X \subseteq \langle X\rangle \leq G$. Entonces todo elemento de la forma $x_1^{n_1}\cdots x_k^{n_k}$ con $x_j \in X$ pertenece a $\langle X\rangle$. Por lo tanto, $U \subseteq \langle X\rangle$.

(2) Dado que $x_ix_j = x_jx_i$ para todo $i, j \in \{1, \ldots, m\}$, se sigue que $x_j^{-1}x_i = x_ix_j^{-1}$, y de estas dos por inversión se tiene que $x_j^{-1}x_i^{-1} = x_i^{-1}x_j^{-1}$ y $x_i^{-1}x_j = x_jx_i^{-1}$. Usando inducción

matemática se sigue que todas las potencias de x_i conmutan con todas las potencias de x_j para todo $i, j \in \{1, \ldots, m\}$.

(3) Se sigue de (2).

(4) Se deja como ejercicio. □

1.2.15 Observación. Sea G un grupo y $\varnothing \neq X \subseteq G$. Dado que $\langle X \rangle$ es una intersección de subgrupos, se sigue que $\langle X \rangle$ es un subgrupo de G, y si U es un subgrupo cualquiera de G que contiene a X, entonces $\langle X \rangle$ es un subgrupo de U, por lo tanto, $\langle X \rangle$ es el subgrupo mínimo de G que contiene a X.

1.2.16 Ejemplos. (1) Si G es un grupo y $U \leq G$, entonces $\langle \varnothing \rangle = 1$ y $\langle U \rangle = U$.

(2) El grupo $\mathbb{Z}$ es cíclico. En efecto, $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.

(3) El grupo $U(n)$ de las raíces n-ésimas complejas de la unidad satisface que $U(n) = \langle \zeta_n \rangle$.

(4) Si $V = \{1, g, h, k\}$ es el 4-grupo de Klein (ver ejemplo 1.1.5), entonces se tiene que $V = \langle g, h \rangle = \langle g, k \rangle = \langle h, k \rangle$. Es decir, V es finitamente generado, pero no es cíclico.

(5) El grupo simétrico de grado 3 es finitamente generado y no cíclico. Se cumple que $\mathrm{Sym}(3) = \langle (12), (123) \rangle$.

1.2.17 Ejemplo. (Grupo dihédrico o diedral de grado n) Sea $n \geq 3$ y consideremos nuevamente el conjunto $U(n)$ de las n-esimas raíces complejas de la unidad. Se demostró anteriormente que $U(n)$ es un subgrupo del grupo multiplicativo de $\mathbb{C}$. Sean α y β permutaciones de $U(n)$ definidas por $\alpha(z) := z^{-1}$ y $\beta(z) := \zeta_n z$. (Ver figura 1.3)

Note que $\alpha(z)$ es la reflexión de z con respecto al eje x, mientras que $\beta(z)$ es la rotación de z un ángulo de $2\pi/n$ en sentido antihorario. En consecuencia, $\alpha^2 = \beta^n = (1)$. Esto también puede verificarse analíticamente. De $\alpha^2 = (1)$ se sigue que $\alpha^{-1} = \alpha$.

Note además que para todo $x \in U(n)$

$$\alpha\beta\alpha^{-1}(x) = \alpha\beta(\alpha^{-1}(x)) = \alpha\beta(\alpha(x)) = \alpha(\beta(x^{-1})) = \alpha(\zeta_n x^{-1}) = \zeta_n^{-1} x.$$

Por otro lado para todo $x \in U(n)$ se tiene que $\beta(\zeta_n^{-1} x) = \zeta_n \zeta_n^{-1} x = x$. Es decir, $\beta^{-1}(x) = \zeta_n^{-1} x$. Esto demuestra que

$$\alpha\beta\alpha^{-1} = \beta^{-1}. \tag{1.4}$$

Definamos $D_{2n} := \langle \alpha, \beta \rangle \subseteq \mathrm{Sym}(U(n))$. Dado que $\beta \neq \beta^{-1}$, se sigue que D_{2n} es un grupo no abeliano y consecuencia de (1.4) se tienen entonces las siguientes relaciones:

$$\alpha\beta = \beta^{-1}\alpha \quad \text{y} \quad \beta\alpha = \alpha\beta^{-1}. \tag{1.5}$$

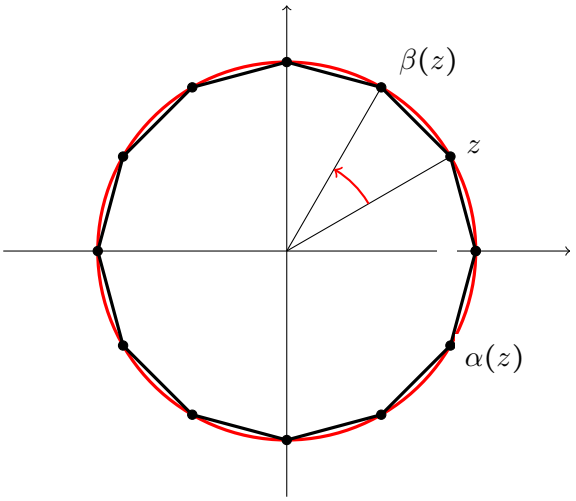


Figura 1.3: Generadores del grupo dihédrico de grado n

Si $\rho \in D_{2n}$, entonces $\rho = \rho_1^{\varepsilon_1} \cdots \rho_k^{\varepsilon_k}$, con $k \in \mathbb{N}$, $\varepsilon_j \in \mathbb{Z}$ y $\rho_j \in \{\alpha, \beta\}$. Usando (1.5) y el hecho de que $\alpha^2 = \beta^n = (1)$ se sigue que

$$D_{2n} = \{\alpha^i \beta^j \mid i, j \in \mathbb{Z}\} = \{\alpha^i \beta^j \mid 0 \leq i \leq 1,\ 0 \leq j \leq n-1\}.$$

Demostramos ahora que estos $2n$ elementos son distintos. Supongamos que $\alpha^i \beta^j = \alpha^r \beta^s$, para $i, r \in \{0, 1\}$ y $j, s \in \{0, 1, \ldots, n-1\}$. Si $i = r$, entonces claramente $j = s$. Sea entonces $i \neq r$, y sin perder generalidad supongamos que $i = 0$ y $r = 1$. Entonces $\alpha = \beta^{j-s}$, y así

$$\begin{aligned} x^{-1} &= \alpha(x) \\ &= \beta^{j-s}(x) \\ &= \zeta_n^{j-s} x, \end{aligned}$$

para todo $x \in U(n)$. Es decir, $\zeta_n^{j-s} x^2 = 1$, $\forall x \in U(n)$, lo cual no es posible. En consecuencia, $i = r$, y por lo tanto $j = s$. El grupo D_{2n} se denomina `dihédrico o diedral` de grado n.

1.2.18 Ejemplo. (El grupo de simetrías de un triángulo) Como caso particular sea $n = 3$. Entonces se tiene que $U(3) = \{1, \zeta_3, \zeta_3^2\}$, como se observa en la figura 1.4.

Identificamos el conjunto $U(3)$ con $\Omega = \{1, 2, 3\}$, como se muestra en la figura 1.5, y consideramos los siguientes movimientos que dejan fijo el triángulo:

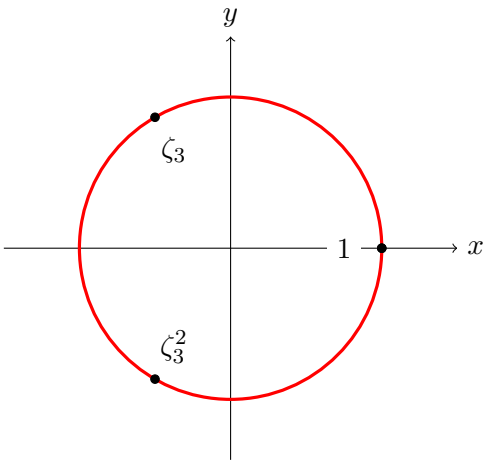


Figura 1.4: Raíces 3-ésimas o cúbicas de la unidad

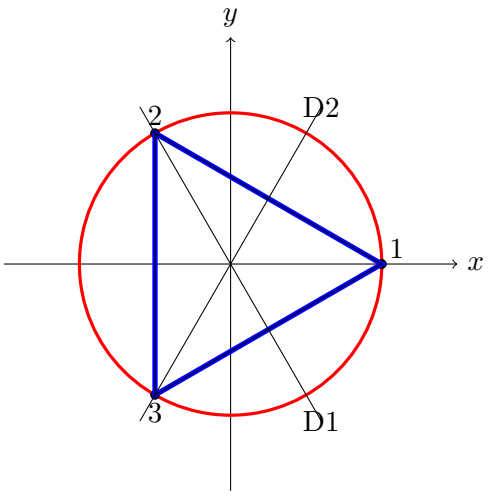


Figura 1.5: Simetrías del triángulo

- No moverlo. Aunque parezca contradictorio, ¡matemáticamente puede considerarse como un movimiento!
- Reflexión con respecto al eje x. Asociemos a este movimiento la permutación α. Es decir, $\alpha = (23) \in \mathrm{Sym}(3)$.
- Una rotación de 120 o 240 grados con respecto al centro. Identificamos la rotación de 120 grados con la permutación β. Es decir, $\beta = (123) \in \mathrm{Sym}(3)$.

- Las simetrías con respecto a las diagonales D1 y D2.

Estos seis movimientos tienen asociadas exactamente los seis elementos del grupo simétrico Sym(3). Esto es,

$$\{(1), (23), (123), (132), (13), (12)\}.$$

1.2.19 Ejemplo. (D_8-El grupo de simetrías del cuadrado) Consideremos ahora $n = 4$ e identifiquemos $U(4) = \{1, i, -1, -i\}$ con el conjunto $\Omega = \{1, 2, 3, 4\}$, como se muestra en la figura 1.6.

Los siguientes movimientos que dejan fijo al cuadrado:

- No moverlo.
- Reflexión con respecto al eje x. Asociemos a este movimiento la permutación α. Es decir, $\alpha = (24) \in \text{Sym}(4)$.
- Reflexión con respecto al eje y.
- Una rotación de 90, 180 o 270 grados con respecto al centro. Identificamos la rotación de 90 grados con la permutación β. Es decir, $\beta = (1234) \in \text{Sym}(4)$.
- Las simetrías con respecto a las diagonales D1 y D2.

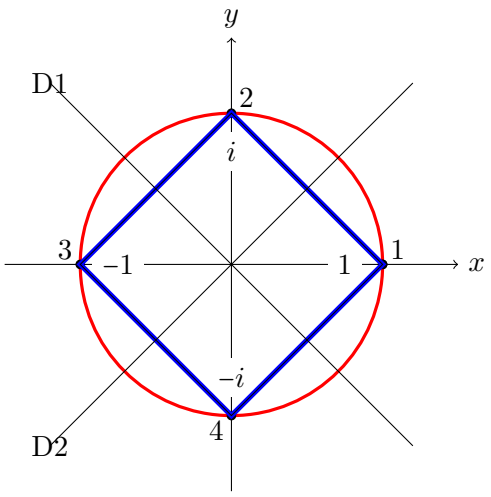


Figura 1.6: Simetrías del cuadrado

Estos ocho movimientos tienen asociadas las siguientes permutaciones en el grupo simétrico Sym(4):

- La función identidad (1),
- $\alpha = (24)$,
- $\gamma = (13) = \alpha\beta^2$,
- $\beta = (1234)$,
- $\beta^2 = (13)(24)$,
- $\beta^3 = (1432)$,
- $\delta = (14)(23) = \alpha\beta$,
- $\eta = (12)(34) = \alpha\beta^3$.

Estas permutaciones corresponden al grupo D_8, el cual sabemos está dado por

$$D_8 = \{(1), \alpha, \alpha\beta, \alpha\beta^2, \alpha\beta^3, \beta, \beta^2, \beta^3\}.$$

Se puede verificar sin mayores dificultades la siguiente tabla de multiplicación:

$\circ$	(1)	α	$\alpha\beta$	$\alpha\beta^2$	$\alpha\beta^3$	β	β^2	β^3
(1)	(1)	α	$\alpha\beta$	$\alpha\beta^2$	$\alpha\beta^3$	β	β^2	β^3
α	α	(1)	β	β^2	β^3	$\alpha\beta$	$\alpha\beta^2$	$\alpha\beta^3$
$\alpha\beta$	$\alpha\beta$	β^3	(1)	β	β^2	$\alpha\beta^2$	$\alpha\beta^3$	α
$\alpha\beta^2$	$\alpha\beta^2$	β^2	β^3	(1)	β	$\alpha\beta^3$	α	$\alpha\beta$
$\alpha\beta^3$	$\alpha\beta^3$	β	β^2	β^3	(1)	α	$\alpha\beta$	$\alpha\beta^2$
β	β	$\alpha\beta^3$	α	$\alpha\beta$	$\alpha\beta^2$	β^2	β^3	(1)
β^2	β^2	$\alpha\beta^2$	$\alpha\beta^3$	α	$\alpha\beta$	β^3	(1)	β
β^3	β^3	$\alpha\beta$	$\alpha\beta^2$	$\alpha\beta^3$	α	(1)	β	β^2

Tabla 1.2: Tabla de multiplicación del grupo D_8

1.2.20 Ejemplo. (El grupo de los cuaterniones) Consideremos las matrices

$$x := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad y := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{C}).$$

Teniendo como operación la multiplicación de matrices, definamos el grupo $\mathbb{Q}_8$ de la siguiente manera:

$$\mathbb{Q}_8 := \langle x, y \rangle \subset \mathrm{GL}_2(\mathbb{C}).$$

Este grupo es denominado el grupo de los `cuaterniones`. Note que

$$\begin{aligned}
x^2 &= \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \\
y^2 &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \\
xy &= \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \\
(xy)^2 &= \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}
\end{aligned}$$

Entonces

$$x^2 = y^2 = (xy)^2.$$

Por otro lado,

$$\begin{aligned}
x^4 &= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\
yx &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \\
x^{-1}y &= \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}
\end{aligned}$$

En consecuencia,

$$x^4 = 1,\ x^2 = y^2 = (xy)^2 \quad \text{y} \quad yxy^{-1} = x^{-1}. \tag{1.6}$$

Si $z \in \mathbb{Q}_8$, entonces $z = z_1^{\varepsilon_1} \cdots z_k^{\varepsilon_k}$, con $k \in \mathbb{N}$, $\varepsilon_j \in \mathbb{Z}$ y $z_j \in \{x, y\}$. Utilizando las relaciones (1.6) se obtiene que

$$\begin{aligned}
\mathbb{Q}_8 &= \{x^i y^j \mid i, j \in \mathbb{Z}\} \\
&= \{x^i y^j \mid 0 \le i \le 3,\ 0 \le j \le 3\} \\
&= \{1, y, y^2, y^3, x, xy, xy^2, xy^3, x^2, x^2y, x^2y^2, x^2y^3, x^3, x^3y, x^3y^2, x^3y^3\}.
\end{aligned}$$

No obstante, no todos estos elementos son distintos. Usando nuevamente las relaciones (1.6) concluimos que

$$\mathbb{Q}_8 = \{1, x, x^2, x^3, y, y^3, xy, yx\}.$$

Note $xy \neq yx$, por lo tanto, $\mathbb{Q}_8$ es un grupo no abeliano. Su tabla de multiplicación se presenta a continuación:

$\cdot$	1	x	x^2	x^3	y	y^3	xy	yx
1	1	x	x^2	x^3	y	y^3	xy	yx
x	x	x^2	x^3	1	xy	yx	y^3	y
x^2	x^2	x^3	1	x	y^3	y	yx	xy
x^3	x^3	1	x	x^2	yx	xy	y	y^3
y	y	yx	y^3	xy	x^2	1	x	x^3
y^3	y^3	xy	y	yx	1	x^2	x^3	x
xy	xy	y	yx	y^3	x^3	x	x^2	1
yx	yx	y^3	xy	y	x	x^3	1	x^2

Tabla 1.3: Tabla de multiplicación del grupo de los cuaterniones

Un problema interesante de la teoría de grupos ha sido siempre construir grupos a partir de otros grupos dados o mediante el análisis de la estructura interna de un grupo dado. Los próximos resultados nos permiten encontrar nuevas técnicas para construir subgrupos de un grupo G dado.

1.2.21 Definición. Sea G un grupo y $\varnothing \neq U, V \subseteq G$. Definimos y notamos el `producto complejo` o `producto de Frobenius` entre U y V de la siguiente manera:

$$UV := \{uv \mid u \in U,\ v \in V\}.$$

Si $g \in G$, entonces escribimos gU y Ug en lugar de $\{g\}U$ y $U\{g\}$, respectivamente. Estos conjuntos se denominan `clase lateral izquierda` de g con respecto a U, respectivamente `derecha`.

1.2.22 Lema. Sea G un grupo y $\varnothing \neq U, V, W \subseteq G$. Entonces

(1) $UV \subseteq \langle U \cup V \rangle$.

(2) $U \cup V \subseteq UV$.

(3) Si U, V y UV son subgrupos de G, entonces $UV = \langle U \cup V \rangle$. En este caso escribimos simplemente $UV = \langle U, V \rangle$.

(4) $U(VW) = (UV)W$.

(5) Si $U \subseteq V$, entonces $UW \subseteq VW$ y $WU \subseteq WV$.

(6) Si G es abeliano, entonces $UV = VU$.

DEMOSTRACIÓN. (1) Si $x \in UV$, entonces $x = uv$, con $u \in U$ y $v \in V$. Del teorema 1.2.14 (1) se sigue que $x \in \langle U \cup V \rangle$.

(2) Si $x \in U \cup V$, entonces $x \in U$ o $x \in V$. Dado que $1 \in U \cap V$, se sigue que $x = x1 = 1x \in UV$.

(3) Es suficiente demostrar que $\langle U \cup V \rangle \subseteq UV$, ya que la otra contenencia se sigue de (1). Por hipótesis $UV \leq G$ y de (2) se sigue que $U \cup V \subseteq UV$. Usando la observación 1.2.15 se tiene la conclusión.

(4) Se sigue inmediatamente de la asociatividad de la multiplicación en G.

(5) Se sigue inmediatamente de la definición de producto complejo.

(6) Se deja como ejercicio. □

1.2.23 Observaciones. Sea G un grupo y $U, V \leq G$.

(1) En general no es cierto que $UV \leq G$. Por ejemplo, si $G = \mathrm{Sym}(3)$, $U := \{(1), (23)\}$ y $V := \{(1), (13)\}$, entonces $UV = \{(1), (23), (13), (123)\} \nleq G$.

(2) De $UV = VU$ no necesariamente se sigue que $uv = vu$ para todo $u \in U$ y $v \in V$. Esta afirmación solo dice que dado $uv \in UV$, es posible encontrar $u' \in U$ y $v' \in V$ tales que $uv = v'u'$.

1.2.24 Teorema. Sea G un grupo y $U, V \leq G$. Entonces $UV \leq G$ si y solo si $VU \subseteq UV$.

DEMOSTRACIÓN. Supongamos que $UV \leq G$. Entonces $VU \subseteq UVUV = UV$.

Recíprocamente, supongamos que $VU \subseteq UV$ y sean $u_1v_1, u_2v_2 \in UV$. Entonces

$$\begin{aligned} u_1v_1(u_2v_2)^{-1} &= u_1 \underbrace{v_1v_2^{-1}}_{=v_3 \in V} u_2^{-1} \\ &= u_1 \underbrace{v_3u_2^{-1}}_{\in VU} \\ &= \underbrace{u_1u_3}_{=u \in U} v_4 \\ &= uv_4. \end{aligned}$$

En consecuencia, $u_1v_1(u_2v_2)^{-1} \in UV$ y del teorema 1.2.3 se tiene que $UV \leq G$. □

1.2.25 Definición. Sea G un grupo y $\varnothing \neq U \subseteq G$. Definimos $U^{-1} := \{u^{-1} \mid u \in U\}$.

El siguiente lema determina algunas propiedades de esta operación.

1.2.26 Lema. Sea G un grupo y $\varnothing \neq U, V \subseteq G$. Entonces

(1) $(U^{-1})^{-1} = U$.

(2) $(UV)^{-1} = V^{-1}U^{-1}$.

Demostración. (1) $(U^{-1})^{-1} = \{x^{-1} \mid x \in U^{-1}\} = \{(u^{-1})^{-1} \mid u \in U\} = \{u \mid u \in U\} = U$.

(2) $(UV)^{-1} = \{(uv)^{-1} \mid u \in U,\ v \in V\} = \{v^{-1}u^{-1} \mid u \in U,\ v \in V\} = V^{-1}U^{-1}$. □

1.2.27 Lema. Sea G un grupo y $\varnothing \neq X \subseteq U \leq G$. Entonces

(1) $U^{-1} = U$.

(2) $XU = UX = U$. En particular $UU = U$ y $uU = Uu = U$ para todo $u \in U$.

Demostración. (1) Supongamos que $U \leq G$. Entonces

$$\begin{aligned} x \in U^{-1} &\Leftrightarrow x = u^{-1} \text{ para algún } u \in U \\ &\Leftrightarrow x = u' \text{ para algún } u' \in U \\ &\Leftrightarrow x \in U. \end{aligned}$$

(2) Se deja como ejercicio. □

1.2.28 Observación. El recíproco de la afirmación (3) en el lema anterior es en general falso. Por ejemplo, si V es un subgrupo no trivial de G y definimos $U := V \setminus \{1\}$, entonces $U^{-1} = U$ y no se verifica que $U \leq G$.

1.2.29 Lema. (Identidad de Dedekind) Sea G un grupo y $U, V, W \leq G$, con $V \leq U$. Entonces

$$U \cap VW = V(U \cap W).$$

Demostración. Dado que $V \subseteq U, VW$ y $U \cap W \subseteq U, VW$, se sigue que $V(U \cap W) \subseteq U \cap VW$.

Recíprocamente,

$$\begin{aligned} x \in U \cap VW &\Leftrightarrow x = u = vw, \text{ con } u \in U,\ v \in V,\ w \in W \\ &\Rightarrow w = v^{-1}u \in VU = U \\ &\Rightarrow w \in U \cap W \\ &\Rightarrow x = vw \in V(U \cap W), \end{aligned}$$

con lo cual se tiene la afirmación. □

1.3 Clases laterales y transversales

A lo largo de esta sección G denota siempre un grupo.

Demostramos a continuación que el orden de todo subgrupo U divide al orden de G, siempre que G sea finito. Listamos a continuación algunas propiedades de las clases laterales de U en G.

1.3.1 Lema. Sea $U \leq G$. Definamos sobre G la siguiente relación:

$$g \sim_U h \Leftrightarrow g^{-1}h \in U.$$

Entonces $\sim_U$ es una relación de equivalencia sobre G y la clase de equivalencia de $g \in G$ tiene la forma gU. Es decir, las clase laterales izquierdas de U en G.

Demostración. Se deja como ejercicio. □

1.3.2 Observación. De manera similar, la relación

$$g \sim^U h \Leftrightarrow gh^{-1} \in U$$

es de equivalencia sobre G y determina las clases laterales derechas de U en G.

Listamos a continuación algunas propiedades de las clases laterales, las cuales son consecuencias inmediata del lema anterior.

1.3.3 Lema. Sea $U \leq G$ y $g, h \in G$. Entonces

(1) $gU = hU$ si y solo si $g^{-1}h \in U$

(2) $gU = U$ si y solo si $g \in U$

(3) $gU \neq hU$ si y solo si $gU \cap hU = \varnothing$

(4) $G = \bigcup_{g \in G} gU$

(5) $|gU| = |U| = |Ug|$ para todo $g \in G$.

(6) El conjunto de las clases laterales izquierdas de U en G y el conjunto de las clases laterales derechas de U en G tienen el mismo número de elementos.

Demostración. Las primeras cuatro afirmaciones son consecuencia del hecho que $\sim_U$ es de equivalencia. No obstante reescribimos sus demostraciones.

(1) Supongamos que $gU = hU$. Entonces $gu_1 = hu_2$ para $u_1, u_2 \in U$ y se tiene que $g^{-1}h = u_1u_2^{-1} \in U$.

Recíprocamente, si $g^{-1}h \in U$, entonces del lema 1.2.27 (2) se sigue que $g^{-1}hU = U$ y, en consecuencia, $gU = hU$.

(2) Se sigue de (1).

(3) Supongamos que existe $x = gu_1 = hu_2 \in gU \cap hU$, donde $u_1, u_2 \in U$. Entonces $g = hu_2u_1^{-1}$ y se tiene que $gU = hu_2u_1^{-1}U$. Dado que $u_2u_1^{-1} \in U$, podemos usar nuevamente 1.2.27 (2) y se tiene que $hu_2u_1^{-1}U = hU$. Por lo tanto, $gU = hU$.

Recíprocamente, si $gU \cap hU = \varnothing$, entonces claramente $gU \neq hU$.

(4) Si $g \in G$, entonces $g \in gU$ y se tiene la afirmación.

(5) Las funciones $\varphi : U \longrightarrow gU$ y $\psi : U \longrightarrow Ug$, definidas, respectivamente, por $\varphi(x) = gx$ y $\psi(x) = xg$, son biyectivas.

(6) Sean $L = \{gU \mid g \in G\}$ y $R = \{Ug \mid g \in G\}$. Definamos $\varphi : L \longrightarrow R$ mediante $\varphi(gU) \coloneqq Ug^{-1}$.

`Afirmación.` φ es una biyectiva.

Note que

$$gU = hU \Leftrightarrow U^{-1}g^{-1} = U^{-1}h^{-1} \Leftrightarrow Ug^{-1} = Uh^{-1}.$$

Esto demuestra que φ está bien definida y además es inyectiva. Por otro lado, dado que $\varphi(g^{-1}U) = Ug$, se sigue que φ es sobreyectiva. □

1.3.4 Observación. Como consecuencia del lema anterior existe una descomposición de G en clases laterales izquierdas disyuntas. Es decir, existe $T \subseteq G$ tal que

$$G = \bigcup_{g \in T}^{\cdot} gU. \tag{1.7}$$

Es decir, $G = TU$ y para todo $g, h \in T$ con $g \neq h$ se verifica que $gU \neq hU$.

Esta partición (1.7) se denomina la `descomposición` de G en clases laterales izquierdas con respecto a U. Un conjunto T con tales características se denomina un `transversal izquierdo` de U en G o también un `sistema de representantes` para las clases laterales. De manera similar se define un `transversal derecho`.

1.3.5 Definición. Sea $U \leq G$. Si T es un transversal izquierdo finito de U en G, entonces $|T|$ se llama el `índice` de U en G y lo notamos con $|G : U|$. Si el índice no es finito, entonces escribimos $|G : U| = \infty$.

1.3.6 Ejemplos. (1) Es claro que $|G : G| = 1$ y $|G : 1| = |G|$.

(2) Sea $G = \mathrm{Sym}(3)$, $U = \{(1), (13)\}$, $g = (12)$ y $h = (23)$. Se verifica que U es un subgrupo de G, y además $gU = \{(12), (132)\}$ y $hU = \{(23), (123)\}$. Note que

$$\begin{aligned} G &= \{(1), (12), (23), (13), (123), (132)\} \\ &= \{(1), (13)\} \cup \{(12), (132)\} \cup \{(23), (123)\} \\ &= U \cup gU \cup hU. \end{aligned}$$

En consecuencia, $T = \{(1), (12), (23)\}$ es un transversal izquierdo de U en G. Por lo tanto, $|G : U| = 3$. Se verifica sin dificultades que $gU \neq Ug$.

(3) $T := \{0, 1, \ldots, n-1\}$ es un transversal izquierdo de $n\mathbb{Z}$ en $\mathbb{Z}$. En efecto,

- $T \subseteq G$
- $G = \biguplus_{t \in T} \ t + U$
- Para todo $j, k \in T$ con $j \neq k$ se verifica que $j + U \neq k + U$. Note que

$$j + n\mathbb{Z} = k + n\mathbb{Z} \iff (j - k) \in n\mathbb{Z} \iff j \in k + n\mathbb{Z}.$$

Por lo tanto, $|\mathbb{Z} : n\mathbb{Z}| = n$.

(4) Para el grupo D_8 de simetrías del cuadrado se verifica que $T = \{1, \alpha\}$ es un transversal izquierdo de $U = \{1, \beta, \beta^2, \beta^3\}$. Entonces $|D_8 : U| = 2$.

1.3.7 Teorema. Sean $U, V \leq G$.

(1) Si T es un transversal izquierdo finito de U en G y si S es un transversal izquierdo finito de V en U, entonces TS es un transversal izquierdo finito de V en G y además

(a) $|TS| = |T||S|$

(b) $|G : V| = |G : U||U : V|$.

(2) (`Lagrange`) $|G| = |G : U| \cdot |U|$. En particular, si G es un grupo finito, entonces $|U|$ y $|G : U|$ son divisores de $|G|$.

Demostración. (1) Dado que T es un transversal izquierdo finito de U en G y que S lo es para V en U, se tiene que $G = TU$ y $U = SV$. Por lo tanto, $G = TSV$. Resta entonces demostrar que si $tsV = t's'V$, entonces $ts = t's'$, donde $t, t' \in T$ y $s, s' \in S$.

Dado que $sV \subseteq U$, se sigue con ayuda del lema 1.2.27 (2) que $sVU = U$ y de la misma manera que $s'VU = U$. Si $tsV = t's'V$, se sigue que

$$tU = tsVU = t's'VU = t'U,$$

lo cual trae como consecuencia que $t = t'$. Entonces $sV = s'V$, y con esto se sigue que $s = s'$. Es decir, $ts = t's'$, y se tiene que TS es un transversal izquierdo de V en G, y además

$$\begin{aligned} |G : V| &= |TS| \\ &= |T||S| \\ &= |G : U||U : V|. \end{aligned}$$

(2) Se sigue inmediatamente de (1), tomando $V = 1$. □

1.3.8 Observación. El teorema de Lagrange impone una restricción al orden de todo subgrupo de un grupo dado G. Por ejemplo, el grupo Sym(3) solo puede tener eventualmente subgrupos de orden 1, 2, 3 y 6.

1.3.9 Teorema. Sean $U, V \leq G$. Si T un transversal izquierdo de $U \cap V$ en U, entonces $UV = \bigcup_{t\in T} tV$ y $tV \cap sV = \varnothing$, para $t, s \in T$ con $t \neq s$. Si U y V son finitos, entonces

$$|UV| = \frac{|U|\ |V|}{|U \cap V|}.$$

Demostración. Sea $uv \in UV$, con $u \in U$ y $v \in V$. Dado que $U = \bigcup_{t\in T} t(U \cap V)$, se tiene que $u = tv'$, con $t \in T$ y $v' \in (U \cap V)$. Entonces $uv = tv'v \in tV$. Esto demuestra que $UV \subseteq \bigcup_{t\in T} tV$. La otra inclusión es trivial, ya que $T \subseteq U$. Entonces

$$UV = \bigcup_{t\in T} tV.$$

Sea ahora $x \in (tV \cap sV)$. Entonces $x = tv = sw$, con $t, s \in T$ y $v, w \in V$. Se sigue entonces $s^{-1}t = wv^{-1} \in (U \cap V)$, por lo tanto, $t(U \cap V) = s(U \cap V)$, y con esto se tiene que $t = s$.

Si U y V son finitos, entonces

$$\begin{aligned} |UV| &= |T|\ |V| \\ &= |U : U \cap V|\ |V| \\ &= \frac{|U|}{|U \cap V|}|V| \\ &= \frac{|U|\ |V|}{|U \cap V|}. \quad \square \end{aligned}$$

1.3.10 Teorema. Sean $U, V \leq G$, con $|G : U|$ y $|G : V|$ finitos. Entonces

(1) $|G : U \cap V| \leq |G : U|\ |G : V|$.

(2) (H. Poincaré[5]) La intersección de un número finito de subgrupos con índices finitos tiene índice finito.

(3) Si G es finito, entonces $|G : U \cap V| = |G : U|\ |G : V|$ si y solo si $G = UV$.

(4) Si G es finito y $\text{mcd}(|G : U|, |G : V|) = 1$, entonces $G = UV$.

Demostración. (1) Del teorema 1.3.9 se tiene:

$$|U : U \cap V| = |UV : V| \leq |G : V|.$$

Del teorema 1.3.7 (1) se sigue que

$$\begin{aligned} |G : U \cap V| &= |G : U|\ |U : U \cap V| \\ &\leq |G : U|\ |G : V|. \end{aligned}$$

(2) Se sigue de (1).

(3) Sea G finito. La igualdad $|G : U \cap V| = |G : U|\ |G : V|$ significa que

$$\frac{|G|}{|U \cap V|} = \frac{|G|}{|U|}\frac{|G|}{|V|} = \frac{|G|^2}{|U|\ |V|}.$$

Usando el teorema 1.3.9 obtenemos:

$$|G| = \frac{|U|\ |V|}{|U \cap V|} = |UV|.$$

(4) Dado que $|G : U \cap V| = |G : U||U : U \cap V|$, se sigue que $|G : U|$ divide a $|G : U \cap V|$.

Similarmente se tiene que $|G : V|$ divide a $|G : U \cap V|$.

Por hipótesis

$$\text{mcd}(|G : U|, |G : V|) = 1.$$

Por lo tanto, $|G : U||G : V|$ divide a $|G : U \cap V|$.

De (1) se sigue que

$$|G : U \cap V| = |G : U||U : U \cap V|.$$

Usando (3) se sigue que $G = UV$. □

[5]Henri Poincaré (Nancy, Francia, 1854-París, 1912), matemático francés. Profesor de física matemática en La Sorbona. Trabajó en ecuaciones diferenciales lineales, topología, óptica, electricidad, telegrafía, capilaridad, elasticidad, termodinámica, macánica cuántica, teoría de la relatividad y cosmología.

1.4 Grupos finitos hasta orden 5

Utilizando la teoría desarrollada hasta ahora es posible determinar todos los grupos finitos con orden menor o igual a 4.

- `Grupos de orden 1.` Si $|G| = 1$, entonces $G = \{1\}$, con $11 = 1$.
- `Grupos de orden 2.` Si $|G| = 2$, entonces $G = \{1, g\}$, con $g^2 = gg = 1$.
- `Grupos de orden 3.` Sea $|G| = 3$, digamos $G = \{1, g, h\}$. Dado que $g^2 = gg \neq g$, se verifica que $g^2 \in \{1, h\}$. Si $g^2 = 1$, entonces $gh \neq 1, g, h$ y se tiene un contradicción. Por lo tanto, $g^2 = h$.

  Nuevamente por la propiedad cancelativa se tiene que $gh \neq g, h$ y $hg \neq g, h$. Es decir, forzosamente $gh = hg = 1$. Finalmente, $h^2 \neq h, 1$. En consecuencia, $h^2 = g$.

  La tabla de la multiplicación en G está dada por

$\cdot$	1	g	h
1	1	g	h
g	g	h	1
h	h	1	g

  Note que G es un grupo cíclico, generado por g. Esto es, $G = \{1, g, g^2\}$.

- `Grupos de orden 4.` Sea $|G| = 4$, digamos $G = \{1, g, h, k\}$. En todo grupo de orden par existe por lo menos un $1 \neq x \in G$ tal que $xx = 1$. En efecto, es suficiente agrupar los elementos de G en parejas del tipo (x, x^{-1}), con $x \neq x^{-1}$. Dado que G tiene orden par y $11 = 1$ se sigue que existe por lo menos un $x \neq 1$ con $x = x^{-1}$.

  Supongamos que $g^2 = 1$. Entonces tenemos inicialmente la tabla

$\cdot$	1	g	h	k
1	1	g	h	k
g	g	1		
h	h			
k	k			

  Observemos ahora que $gh \neq 1, g, h$. Es decir, necesariamente $gh = k$. De manera similar se obtiene que $hg = k$. Como consecuencia, $gk = kg = h$. Entonces tenemos

$\cdot$	1	g	h	k
1	1	g	h	k
g	g	1	k	h
h	h	k		
k	k	h		

Para $h^2 = hh$ existen dos posibilidades: $h^2 = 1$ o $h^2 = g$.

(1) Si $h^2 = hh = 1$, entonces $hk, kh \neq h, k, 1$. Es decir, solo permanece libre

$$hk = kh = g.$$

Finalmente $k^2 = kk = 1$ y se tiene en definitiva el denominado `4-grupo de Klein`

$\cdot$	1	g	h	k
1	1	g	h	k
g	g	1	k	h
h	h	k	1	g
k	k	h	g	1

Note que cada elemento de G es su propio inverso.

(2) Si $h^2 = g$, entonces $hk, kh \neq h, k, g$. Es decir, solo permanece libre

$$hk = kh = 1.$$

Finalmente $kk = g$ y se tiene

$\cdot$	1	g	h	k
1	1	g	h	k
g	g	1	k	h
h	h	k	g	1
k	k	h	1	g

Hemos encontrado entonces que solo existen dos grupos abelianos distintos de orden 4.

- `Grupos de orden 5.` Sea $|G| = 5$. Del teorema de Lagrange se sigue que G solo admite subgrupos triviales. Por otro lado, todos los elementos de G tienen orden finito. Esto implica que solo es posible elementos con orden 1 o 5, ya que de lo contrario existirían subgrupos no triviales.

  En conclusión, existe $g \in G$ con $\text{ord}(g) = 5$. Por lo tanto, $G = \{1, g, g^2, g^3, g^4\}$ y se tiene

$\cdot$	1	g	g^2	g^3	g^4
1	1	g	g^2	g^3	g^4
g	g	g^2	g^3	g^4	1
g^2	g^2	g^3	g^4	1	g
g^3	g^3	g^4	1	g	g^2
g^4	g^4	1	g	g^2	g^3

1.5 Ejercicios

1. En cada caso indique cuál axioma de la definición de grupo no se verifica:

   (a) Sea $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$. Entonces $(\mathbb{N}_0, +)$ y $(\mathbb{N}_0, \cdot)$ no son grupos.

   (b) Sea $\mathscr{P}(X)$ el conjunto potencia de un conjunto no vacío X. Entonces $(\mathscr{P}(X), \cup)$ y $(\mathscr{P}(X), \cap)$ no son grupos.

   (c) Sobre el conjunto $\mathbb{Q}$ de los números racionales definamos la siguiente operación binaria:

   $$x \cdot y := x + y + xy.$$

   Entonces $(\mathbb{Q}, \cdot)$ no es un grupo.

   (d) Sea X un conjunto no vacío y $\mathrm{Fun}(X)$ el conjunto de las funciones de X en X. Entonces $\mathrm{Fun}(X)$ con la composición de funciones como operación no es un grupo.

   (e) Sea $K[x]$ el conjunto de los polinomios con coeficientes en un cuerpo K. Entonces $(K[x], \cdot)$ no es un grupo.

   (f) Sea $\mathrm{Mat}(n, \mathbb{R})$ el conjunto de las matrices de tamaño $n \times n$ con entradas reales. Entonces $\mathrm{Mat}(n, \mathbb{R})$ con la multiplicación usual de matrices no es un grupo.

2. Sea G un conjunto no vacío y $(x, y) \longmapsto x \cdot y$ una operación binaria sobre G. La pareja $(G, \cdot)$ se denomina un `monoide` si $\cdot$ es asociativa y admite un elemento identidad.

   Sea G un monoide y $\varnothing \neq U \subseteq G$. Decimos que U es un `submonoide` de G si para todo $x, y \in U$ se verifica que $xy \in U$ y $1 \in U$. Es decir. Usamos la notación $U \leq G$.

   Sea G un monoide. Se dice que $g \in G$ es `cancelable a izquierda` si de $gh = gh'$ se sigue que $h = h'$, y decimos que $g \in G$ es `cancelable a derecha` si de $hg = h'g$ se sigue que $h = h'$. Demuestre que el subconjunto de G formado por los elementos que son cancelables a izquierda es un submonoide de G. Por supuesto, también lo es el subconjunto de G formado por los elementos que son cancelables a derecha.

3. Dada una familia $\{U_i\}_{i \in I}$ de submonoides de un monoide G, demuestre que existe un submonoide mínimo de G, notado $\bigvee_{i \in I} U_i$, que contiene a $\bigcup_{i \in I} U_i$. Para ello demuestre que

   $$\bigvee_{i \in I} U_i = \Big\langle \bigcup_{i \in I} U_i \Big\rangle = \{u_{i_1} \cdots u_{i_n} \mid n \in \mathbb{N}_0,\ i_j \in I,\ i_j \neq i_{j+1},\ u_{i_j} \in U_{i_j}\}.$$

   Demuestre además que si $U_i U_j = U_j U_i$ para todo $i \neq j$ e I es un conjunto totalmente ordenado, entonces

   $$\bigvee_{i \in I} U_i = \{u_{i_1} \cdots u_{i_n} \mid n \in \mathbb{N}_0,\ i_1 < i_2 < \cdots < i_n \in I,\ u_{i_j} \in U_{i_j}\}.$$

4. Demuestre que un semigrupo G es un grupo si y solo si para todo $a, b \in G$ existen únicos $x, y \in G$ tales que $ax = b$ y $ya = b$.

5. Demuestre que un semigrupo finito G es un grupo si y solo si en G se verifican las leyes de cancelación.

6. Demuestre la parte (6) del lema 1.2.22.

7. Demuestre la parte (4) del lema 1.2.27.

8. Defina sobre el conjunto de los número reales $\mathbb{R}$ la siguiente operación binaria:

$$x \cdot y := x + y + xy \qquad \forall\ x, y \in \mathbb{R}$$

   (a) ¿Es $(\mathbb{R}, \cdot)$ un grupo?

   (b) Si no lo es, ¿existe $K \subset \mathbb{R}$ tal que $(K, \cdot)$ sea un grupo?

9. Sea G un grupo y $a \in G$ fijo. Definamos

$$x \cdot y := xay \qquad \text{para todo } \ x, y \in G$$

   Demuestre que $(G, \cdot)$ es también un grupo.

10. `Demuestre o refute:` Sea p un número primo y definamos

$$\mathbb{Q}_p := \left\{ \frac{a}{p^n} \mid a \in \mathbb{Z},\ n \in \mathbb{N}_0 \right\}.$$

    (a) $\mathbb{Q}_p$ es un grupo abeliano con respecto a la suma.

    (b) $\mathbb{Q}_p \setminus \{0\}$ es un grupo con respecto a la multiplicación.

11. `Demuestre o refute:` Sea G un conjunto y $\cdot$ una operación binaria definida sobre G tal que $(G, \cdot)$ no es un grupo. Si $H \subset G$, entonces $(H, \cdot)$ no es un grupo.

12. `Demuestre o refute:` Sea G un grupo finito y abeliano. Entonces

$$\prod_{g \in G} g = 1.$$

13. `Demuestre o refute:` Existe un grupo infinito en el cual todo elemento, salvo el neutro, tiene orden 2.

14. Sea G un grupo. Demuestre que para todo $a, b \in G$ existen únicos $x, y \in G$ tales que $ax = b$ y $ya = b$.

15. Sea G un grupo y $g \in G$. Demuestre que si $g^2 = g$, entonces $g = 1$.

16. Sea G un grupo. Demuestre que si $g^2 = 1$ para todo $g \in G$, entonces G es abeliano.

17. Sea G un grupo finito y abeliano. Demuestre que

$$\prod_{g \in G} g^2 = 1.$$

18. Sea G un grupo que contiene un número finito de subgrupos. Demuestre que G es finito.

19. Sea G un grupo con orden par. Demuestre que:

    (a) G tiene por lo menos un elemento g tal que $g^2 = 1$,

    (b) el número de elementos en G con orden 2 es un número impar.

20. Sean

$$g = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad h = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}).$$

    Determine:

    (a) $\mathrm{ord}(g)$

    (b) $\mathrm{ord}(h)$

    (c) $\mathrm{ord}(gh)$

    (d) $\mathrm{ord}(hg)$

21. Sea G un grupo finito. Demuestre que $|G|$ es un número impar si y solo si para todo $x \in G$ existe $y \in G$ tal que $x = y^2$.

22. Sea G un grupo y $H \leq G$. Para $x, y \in G$ definamos:

$$x \sim y \text{ si y solo si } xy^{-1} \in H.$$

    (a) ¿Define $\sim$ una relación de equivalencia definida sobre G?

    (b) En caso afirmativo, para $g \in G$ determine $[g]$.

23. Sea G un grupo y a un elemento fijo de G. Demuestre que $H_a := \{x \in G \mid xa = ax\}$ es un subgrupo de G.

24. Notemos con $\mathrm{Alt}(4)$ el conjunto de las permutaciones pares de $\mathrm{Sym}(4)$. Es decir,

$$\mathrm{Alt}(4) = \{(1), (12)(34), (13)(24), (14)(23), (123), (132), (234), (243), (341), (314), (412), (421)\}$$

    Demuestre que $\mathrm{Alt}(4) < \mathrm{Sym}(4)$.

25. Para cada uno de los grupos $\mathrm{GL}_2(2)$, $\mathrm{Sym}(3), \mathbb{Q}_8, D_8$ y $\mathrm{Alt}(4)$ determine:

    (a) los órdenes de sus elementos

    (b) todos sus subgrupos.

26. Sea $q \in \mathbb{Q}$ fijo. Demuestre que $(q\mathbb{Z}, +)$ es un subgrupo de $(\mathbb{Q}, +)$.

27. Considere el conjunto G de las funciones reales de variable real definidas de la siguiente manera:

$$T_{a,b}(x) = ax + b,$$

    con $a \neq 0, a, b, \in \mathbb{R}$. Sea

$$H := \{T_{a,b} \mid a = \pm 1,\ b \in \mathbb{R}\}.$$

    ¿Es H un subgrupo de G? (La operación es la composición de funciones).

28. Sea U un subconjunto finito no vacío de un grupo G. Demuestre que $U \leq G$ si y solo si para todo $u, v \in U$ se verifica que $uv \in U$.

29. Consideremos los siguientes subconjuntos de $\mathrm{GL}_2(\mathbb{R})$:

    (a) $U = \left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \middle|\ a, b \in \mathbb{R},\ ac \neq 0 \right\}$

    (b) $V = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \middle|\ a \in \mathbb{R}^\times \right\}$

    (c) $W = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \begin{pmatrix} 0 & a \\ a^{-1} & 0 \end{pmatrix} \middle|\ a \in \mathbb{R}^\times \right\}$.

    Determine cuáles son subgrupos de $\mathrm{GL}_2(\mathbb{R})$.

30. Sea G el grupo definido por

$$G := \left\langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle \subseteq \mathrm{GL}_2(\mathbb{R}).$$

    Halle todos los elementos de G.

31. Sea

$$\mathbb{D}_\infty := \left\langle \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle \subseteq \mathrm{GL}_2(\mathbb{R}).$$

    Demuestre que

$$\mathbb{D}_\infty := \left\{ \begin{pmatrix} \pm 1 & n \\ 0 & 1 \end{pmatrix} \middle|\ n \in \mathbb{Z} \right\}.$$

32. Sea G un grupo y $g \in G$ fijo. Demuestre que $H := \{g^n \mid n \in \mathbb{Z}\}$ es un subgrupo de G y que todo subgrupo de G que tenga a g como elemento contiene a H.

33. Sean Ω un conjunto no vacío y $\varnothing \neq X \subseteq \Omega$. Definamos $U, V \subseteq \mathrm{Sym}(\Omega)$ mediante

$$U := \{\sigma \mid \sigma(X) = X\} \quad \text{y} \quad V := \{\sigma \mid \sigma(x) = x, \ \forall x \in X\}.$$

    (a) Demuestre que $V \leq U \leq \mathrm{Sym}(\Omega)$.

    (b) En particular, si $\Omega = \{1, 2, 3\}$, calcule U y V para $X = \{1, 3\}$ y para $X = \Omega$.

34. Sean $m, n \in \mathbb{Z}$ y $k := \mathrm{mcm}(m, n)$. Demuestre que $m\mathbb{Z} \cap n\mathbb{Z} = k\mathbb{Z}$.

35. Sea G un grupo, con $|G| = p^a m$ y $\mathrm{mcd}(p, m) = 1$. Sean $H, K \leq G$ tales que $K \nsubseteq H$, $|H| = p^a$ y $|K| = p^b$ y $0 < d \leq k$. Demuestre que HK no es un subgrupo de G.

36. Sea G un grupo. Demuestre que

    (a) Si H y L son subgrupos de G, entonces $G \neq H \cup L$

    (b) Si H es un subgrupo propio de G, entonces $\langle G \setminus H \rangle = G$.

37. Sea U un subgrupo de un grupo G. Si T es un transversal izquierdo de U en G, demuestre que T^{-1} es un transversal derecho de U en G.

38. Demuestre que si $q = p^k$, siendo p un primo, entonces

$$|\mathrm{GL}_n(q)| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1}).$$

CAPÍTULO 2

HOMOMORFISMOS DE GRUPOS

El poder de las matemáticas está a menudo en cambiar una cosa en otra,
cambiar la geometría en lenguaje.
(Marcus Peter Francis du Sautoy)

En la teoría de grupos resulta de especial interés la clasificación de estos según su "forma". Observamos en el capítulo anterior que existen dos grupos de orden 4. Podemos preguntarnos si es posible diseñar un mecanismo para diferenciar, en algún sentido, un grupo del otro. También encontramos que el grupo de simetrías del cuadrado, D_8 y el grupo de los cuaterniones, ambos tienen orden 8 y el interrogante anterior permanece vigente en este caso. El mecanismo para establecer tales diferencias de formas entre grupos lo constituyen los homomorfismos.

Otro problema interesante consiste en construir nuevas estructuras algebraicas a partir de una dada. Recordemos que en los espacios vectoriales cualquier subespacio vectorial puede ser usado para construir el espacio cociente. En esto la conmutatividad de la suma es muy importante. En el caso de los grupos la situación es diferente. No siempre el conjunto de las clases laterales de un subgrupo con la operación canónica tiene la estructura de grupo. Esta propiedad deseada se verifica solo para algunos subgrupos especiales, denominados `normales`, los cuales se estudian en este capítulo.

Acordamos ahora que a lo largo de este capítulo G denota un grupo multiplicativo.

2.1 Subgrupos normales y grupo cociente

2.1.1 Definición. Si $g, h \in G$, entonces definimos $g^h := h^{-1}gh$ y llamamos a g^h el `conjugado` de g con h. Si X es un subconjunto no vacío de G, entonces

$$X^g = \{x^g \mid x \in X\} = g^{-1}Xg.$$

Más aún, usamos X^G para denotar el conjunto

$$X^G = \{X^g \mid g \in G\}$$

de conjugados de X en G.

2.1.2 Observación. Si G es no abeliano y $U \leq G$, no siempre se verifica que el producto complejo de dos clases laterales izquierdas de U es otra clase lateral izquierda de U. Por ejemplo, si $U = \{(1), (13)\}$ en Sym(3), entonces para $g = (12)$ y $h = (23)$ se verifica que $gUhU = \{(1), (13), (23), (123)\}$, la cual no es una clase lateral de U.

Examinaremos ahora los subgrupos para los cuales esta propiedad deseable se verifica.

2.1.3 Definición. Un subgrupo N de G se denomina `normal` en G si para todo $g \in G$ se verifica que $N^g \subseteq N$. Usamos la notación $N \trianglelefteq G$. Si N es un subgrupo propio de G, escribimos $N \triangleleft G$.

El siguiente teorema establece una serie de criterios para determinar la normalidad de un subgrupo.

2.1.4 Teorema. Sea $N \leq G$. Las siguientes afirmaciones son equivalentes:

(1) $N \trianglelefteq G$.

(2) $N^g = N$ para todo $g \in G$.

(3) $g^{-1}ng \in N$ para todo $g \in G$ y para todo $n \in N$.

(4) $gN = Ng$ para todo $g \in G$.

(5) $(gN)(hN) = (gh)N$ para todo $g, h \in G$.

Demostración. (1) $\Rightarrow$ (2) Dado que $N \trianglelefteq G$, se tiene que $g^{-1}Ng \subseteq N$ para todo $g \in G$. Esta contenencia también se verifica con g^{-1} en lugar de g, es decir, $gNg^{-1} \subseteq N$. Entonces:

$$N = (g^{-1}g)N(g^{-1}g) = g^{-1}(gNg^{-1})g \subseteq g^{-1}Ng,$$

con lo cual se tiene que $N^g = N$.

(2) $\Rightarrow$ (3). Sean $g \in G, n \in N$, entonces $g^{-1}ng = n^g \in N^g = N$.

(3) $\Rightarrow$ (4). Sea $gn \in gN$, entonces $gn = (gng^{-1})g \in Ng$. Esto demuestra que $gN \subseteq Ng$. Similarmente se demuestra la otra contenencia.

(4) $\Rightarrow$ (5). Sean $g, h \in G$. $(gN)(hN) = g(hN)N = (gh)NN = (gh)N$.

(5) $\Rightarrow$ (1). Sea $g \in G$. Entonces $(g^{-1}N)(gN) = N$ y se sigue que $g^{-1}Ng \subseteq N$. Por lo tanto, $N \trianglelefteq G$. $\square$

2.1.5 Ejemplos. (1) Sea G un grupo. Entonces 1 y G son subgrupos normales de G. Si estos son sus únicos subgrupos normales de G, entonces decimos que G es `simple`.

(2) En un grupo abeliano G todos sus subgrupos son normales

(3) Si $N < G$ y $|G : N| = 2$, entonces $N \triangleleft G$. En efecto, dado que $|G : N| = 2$, se sigue que

$$G = N \cup gN = N \cup Ng,$$

con $g \notin N$. Por lo tanto,

$$gN = G \setminus N = Ng.$$

Del teorema 2.1.4 se sigue que $N \triangleleft G$.

(4) Sea $U = \{(1), (23)\}$ en $\mathrm{Sym}(3)$. Entonces $U \not\trianglelefteq G$.

(5) Sea $\mathrm{Alt}(3) = \{(1), (123), (132)\}$ en $\mathrm{Sym}(3)$. Entonces $\mathrm{Alt}(3) \trianglelefteq \mathrm{Sym}(3)$.

(6) En general, $\mathrm{Alt}(n)$ (el grupo alternante de orden n) tiene índice 2 en $\mathrm{Sym}(n)$. Por lo tanto, $\mathrm{Alt}(n) \triangleleft \mathrm{Sym}(n)$

(7) Sean $D_{2n} = \langle \alpha, \beta \rangle$ el grupo dihédrico presentado en el ejemplo 1.2.17 y $N := \langle \beta \rangle$. Dado que $|D_{2n} : N| = 2$, se verifica que N es normal en D_{2n}.

(8) Si $|G|$ es un número primo p, entonces usando el teorema de Lagrange se tiene que G solo admite subgrupos triviales y, por tanto, solo subgrupos normales triviales. Así G es simple.

(9) Si K un cuerpo, entonces $\mathrm{SL}_n(K) \triangleleft \mathrm{GL}_n(K)$.

2.1.6 Observación. La propiedad (5) del teorema 2.1.4 nos permite definir una operación sobre el conjunto de las clases laterales izquierdas de un subgrupo normal N en G. Demostramos ahora que este conjunto adquiere la estructura de grupo.

2.1.7 Teorema. Sean $N \trianglelefteq G$ y $G/N := \{gN \mid \ g \in G\}$. Se define sobre el conjunto G/N la operación

$$gN \cdot hN = ghN.$$

Entonces G/N es un grupo, el cual llamamos `grupo factor` o `grupo cociente` de G módulo N. Si $|G : N|$ es finito, entonces $|G/N| = |G : N|$.

Demostración. Es claro que la operación está bien definida. La asociatividad es consecuencia inmediata de la asociatividad de la operación en G. Sea $g \in G$. Entonces

$$N(gN) = (1N)(gN) = (1g)N = gN.$$

Esto demuetra que N es el módulo en G/N.

Por otro lado, $g^{-1}N \cdot gN = g^{-1}gN = 1N = N$. Entonces, $(gN)^{-1} = g^{-1}N$, y se tiene que G/N es un grupo. □

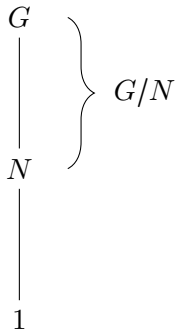


Figura 2.1: El grupo cociente

2.1.8 Ejemplos. (1) Recordemos que $|\mathbb{Z} : n\mathbb{Z}| = n$. Por lo tanto,

$$\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}.$$

(2) Sabemos que $\mathrm{Alt}(3) \trianglelefteq \mathrm{Sym}(3)$. Con unos cálculos simples se tiene que

$$\mathrm{Sym}(3)/\mathrm{Alt}(3) = \{\mathrm{Alt}(3), (12)\mathrm{Alt}(3)\}.$$

En general, $\mathrm{Alt}(n)$ tiene índice 2 en $\mathrm{Sym}(n)$. Por lo tanto, $|\mathrm{Sym}(n)/\mathrm{Alt}(n)| = 2$.

(3) Sean $D_{2n} = \langle \alpha, \beta \rangle$ el grupo dihédrico y $N := \langle \beta \rangle$ se verifica que $N \trianglelefteq D_{2n}$, y además $|D_{2n}/N| = 2$.

(4) Demostramos más adelante que si K es un cuerpo finito con q elementos, entonces $|\mathrm{GL}_n(K)/\mathrm{SL}_n(K)| = q - 1$.

2.1.9 Lema. Sean $N, N_1, N_2 \trianglelefteq G$ y $U \leq G$. Entonces

(1) $U \cap N \trianglelefteq U$.

(2) $UN = NU \leq G$.

(3) $N_1N_2 \trianglelefteq G$.

(4) $N_1 \cap N_2 \trianglelefteq G$.

(5) Si $N_1 \cap N_2 = 1$, entonces $n_1n_2 = n_2n_1$ para todo $n_i \in N_i$.

Demostración:

(1) Sean $u \in U$ y $n \in N \cap U$. Dado que $N \trianglelefteq G$, se verifica que $u^{-1}nu \in N$. De la cerradura de la operación en U se tiene que $u^{-1}nu \in U$. Por lo tanto, $u^{-1}nu \in N \cap U$.

(2) Del teorema 2.1.4 se sigue que $NU = UN$. Es decir, N conmuta con U. Entonces del teorema 1.2.24 se tiene $UN \leq G$.

(3) De (2) se sigue que $N_1N_2 \leq G$. Sean $g \in G$ y $n_i \in N_i$. Entonces

$$g^{-1}n_1n_2g = (g^{-1}n_1g)(g^{-1}n_2g^{-1}) \in N_1N_2.$$

Por lo tanto, $N_1N_2 \trianglelefteq G$.

(4) Claramente $N_1 \cap N_2 \leq G$. Sean $g \in G$ y $n \in N_1 \cap N_2$. Entonces $n \in N_1$ y $n \in N_2$. Dado que $N_i \trianglelefteq G$, se tiene que $g^{-1}ng \in N_1$ y $g^{-1}ng \in N_2$. Por lo tanto, $g^{-1}ng \in N_1 \cap N_2$, lo cual demuestra la normalidad de $N_1 \cap N_2$.

(5) Sean $n_i \in N_i$, con $i = 1, 2$. Entonces

$$n_1^{-1}n_2^{-1}n_1n_2 = n_1^{-1}(n_2^{-1}n_1n_2) \in N_1$$

y también

$$n_1^{-1}n_2^{-1}n_1n_2 = (n_1^{-1}n_2^{-1}n_1)n_2 \in N_2.$$

Por lo tanto,

$$n_1^{-1}n_2^{-1}n_1n_2 \in N_1 \cap N_2$$

y, en consecuencia, $n_1^{-1}n_2^{-1}n_1n_2 = 1$. Finalmente se tiene que $n_1n_2 = n_2n_1$. □

2.2 Homomorfismos

El estudio de grupos y subgrupos hace necesario determinar funciones que preservan la estructura de grupo. Tales funciones son denominadas `homomorfismos`. En lo que sigue nos ocupamos de estudiar homomorfismos entre grupos. Existe una clase especial de homomorfismos, los denominados isomorfismos, los cuales preservan toda la estructura algebraica. Esto es, cualquier afirmación sobre la estructura de G es válida para cualquier grupo isomorfo a G.

2.2.1 Definición. Sean $(G, \cdot)$ y $(H, *)$ dos grupos y $\varphi : G \longrightarrow H$.

(1) Decimos que φ es un `homomorfismo` entre G y H si para todo $x, y \in G$ se verifica

$$\varphi(x \cdot y) = \varphi(x) * \varphi(y).$$

El conjunto de todos los homomorfismos de G en H lo notamos con $\mathrm{Hom}(G, H)$.

(2) $\varphi \in \mathrm{Hom}(G, H)$ se llama un

(a) `monomorfismo` si φ es inyectiva.

(b) `epimorfismo` si φ es sobreyectiva.

(c) `isomorfismo` si φ es biyectiva. Si existe un isomorfismo entre G y H, escribimos $G \cong H$ y decimos que G y H son `isomorfos`.

(d) `endomorfismo` si $G = H$. Escribimos $\mathrm{End}(G)$ en lugar de $\mathrm{Hom}(G, G)$.

(e) `automorfismo` de G si φ es un isomorfismo de G. Con $\mathrm{Aut}(G)$ notamos el conjunto de los isomorfismos de G.

2.2.2 Definición. Sea $\varphi : G \longrightarrow H$ un homomorfismo de grupos. Se notan y definen el `núcleo` y la `imagen` de φ de la siguiente manera:

$$\ker(\varphi) := \{g \in G \mid \varphi(g) = 1\}.$$

$$\mathrm{Im}(\varphi) := \{\varphi(g) \mid g \in G\}.$$

2.2.3 Ejemplos. (1) Para cada $n \in \mathbb{N}$ se verifica que $\varphi : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, +)$ definida por

$$\varphi(x) = nx$$

es un endomorfismo de $\mathbb{Z}$. Además $\ker(\varphi) = 0$ y $\mathrm{Im}(\varphi) = n\mathbb{Z}$.

(2) Sea $\varphi : (\mathbb{R}, +) \longrightarrow ((0, +\infty), \cdot)$ definida por

$$\varphi(x) = e^x.$$

Se verifica que φ es un monomorfismo y además $\mathrm{Im}(\varphi) = (0, +\infty)$.

(3) Sea K un cuerpo con grupo multiplicativo $K^\times$ y $n \in \mathbb{N}$. La función determinante

$$\det : \mathrm{GL}_n(K) \longrightarrow K^\times$$

es un epimorfismo cuyo núcleo es el grupo lineal especial $\mathrm{SL}_n(K)$ sobre K.

2.2.4 Lema. Sea G, H y K grupos.

(1) Si $\varphi : G \longrightarrow H$ y $\psi : H \longrightarrow K$ son homomorfismos, entonces $\psi \circ \varphi$ es un homomorfismo de G en K.

(2) Si $\varphi : G \to H$ es un isomorfismo, entonces $\varphi^{-1} : H \to G$ es un isomorfismo.

Demostración. (1) Sean $x, y \in G$. Entonces

$$\begin{aligned}(\psi \circ \varphi)(xy) &= \psi(\varphi(x)\varphi(y)) \\ &= \psi(\varphi(x))\psi(\varphi(y)) \\ &= (\psi \circ \varphi)(x)(\psi \circ \varphi)(y).\end{aligned}$$

(2) Dado que φ es un isomorfismo, en particular es biyectiva. Entonces para $x, y \in H$ existen $a, b \in G$ tales que $\varphi(a) = x$ y $\varphi(b) = y$. Entonces

$$\begin{aligned}\varphi^{-1}(xy) &= \varphi^{-1}(\varphi(a)\varphi(b)) \\ &= \varphi^{-1}(\varphi(ab)) \\ &= ab \\ &= \varphi^{-1}(x)\varphi^{-1}(y).\end{aligned}$$

Como consecuencia de este lema se tiene que la relación $\cong$ es una relación de equivalencia sobre la clase de todos los grupos.

2.2.5 Ejemplo. (Grupo de Automorfismos interiores) Para $g \in G$ fijo definamos la función $\alpha_g : G \longrightarrow G$ mediante

$$\alpha_g(x) = g^{-1}xg.$$

Se verifica que $\alpha_g \in \mathrm{Aut}(G)$. En efecto, sean $x, y \in G$. Entonces

$$\alpha_g(xy) = g^{-1}(xy)g = (g^{-1}xg)(g^{-1}yg) = \alpha_g(x)\alpha_g(y).$$

Esto demuestra que para cada $g \in G$, la función α_g es un endomorfismo de G. La función $\alpha_{g^{-1}}$ es la inversa de α_g. Por lo tanto, $\alpha_g \in \mathrm{Aut}(G)$. Cada automorfismo de esta forma se denomina un `automorfismo interior` de G. El conjunto

$$\mathrm{Inn}(G) := \{\alpha_g \mid g \in G\}$$

lo llamamos el conjunto de los `automorfismos interiores` de G.

Retornando a la definición de subgrupo normal, podemos afirmar que estos son precisamente aquellos subgrupos de G que son invariantes bajo automorfismos interiores, es decir, la imagen de este bajo un automorfismo interior de G es un subconjunto del subgrupo considerado.

En el siguiente teorema demostramos algunas consecuencias inmediatas de la definición de homomorfismos entre grupos. Si G y H son grupos, no usamos distintivos para sus módulos, escribimos siempre 1 y en el contexto entendemos a cuál hacemos referencia.

2.2.6 Lema. Sean $\alpha \in \mathrm{Hom}(G, H)$, $U \leq G$ y $V \leq H$. Entonces:

(1) $\alpha(1) = 1$.

(2) $\alpha(g^{-1}) = \alpha(g)^{-1}$ para todo $g \in G$.

(3) $\alpha(g^n) = \alpha(g)^n$ para todo $g \in G$ y todo $n \in \mathbb{Z}$.

(4) $\alpha(U) \leq H$. En particular $\mathrm{Im}(\alpha) \leq H$.

(5) $\alpha^{-1}(V) \leq G$.

(6) $\ker(\alpha) \trianglelefteq G$.

Demostración. (1) Note que

$$1\alpha(1) = \alpha(1) = \alpha(1 \cdot 1) = \alpha(1)\alpha(1).$$

En consecuencia, $\alpha(1) = 1$.

(2) Sea $g \in G$. Entonces

$$\alpha(g)\alpha(g^{-1}) = \alpha(gg^{-1}) = \alpha(1) = 1.$$

Por lo tanto, $\alpha(g^{-1}) = \alpha(g)^{-1}$.

(3) Procedemos por inducción sobre n:

(a) Si $n = 1$, entonces la afirmación es inmediata.

(b) Supongamos ahora que $\alpha(g^k) = \alpha(g)^k$ para todo $g \in G$ y para todo $k \in \mathbb{N}$. Entonces

$$\alpha(g^{k+1}) = \alpha(g^k g) = \alpha(g^k)\alpha(g) = \alpha(g)^k\alpha(g) = \alpha(g)^{k+1}.$$

(c) Sea ahora $n < 0$. Entonces $-n \in \mathbb{N}$. Sabemos que $g^n g^{-n} = 1$. Por lo tanto,

$$1 = \alpha(g^n g^{-n}) = \alpha(g^n)\alpha(g^{-n}).$$

Entonces

$$\alpha(g^n) = \alpha(g^{-n})^{-1} = (\alpha(g)^{-n})^{-1} = \alpha(g)^n.$$

(4) Sean $\alpha(g), \alpha(h) \in \alpha(U)$. Entonces

$$\alpha(g)\alpha(h)^{-1} = \alpha(gh^{-1}) \in \alpha(U).$$

(5) Dado que $1 \in \alpha^{-1}(V)$, se sigue que $\alpha^{-1}(V) \neq \varnothing$. Sean $x, y \in \alpha^{-1}(V)$. Entonces

$$\alpha(xy^{-1}) = \alpha(x)\alpha(y)^{-1} \in V.$$

Por lo tanto, $xy^{-1} \in \alpha^{-1}(V)$.

(6) Note que $\ker(\alpha) = \alpha^{-1}(\{1\}) \leq G$. Sean ahora $g \in G$ y $x \in \ker(\alpha)$. Entonces

$$\begin{aligned}\alpha(g^{-1}xg) &= \alpha(g^{-1})\alpha(x)\alpha(g)\\ &= \alpha(g^{-1})1\alpha(g)\\ &= \alpha(g^{-1})\alpha(g)\\ &= 1.\end{aligned}$$

Esto demuestra que $g^{-1}xg \in \ker(\alpha)$. Es decir, $\ker(\alpha) \trianglelefteq G$. □

2.2.7 Lema. Sea $\alpha \in \mathrm{Hom}(G, H)$. Entonces

(1) α es un monomorfismo si y solo si $\ker(\alpha) = 1$.

(2) α es un epimorfismo si y solo si $\mathrm{Im}(\alpha) = H$.

(3) α es un isomorfismo si y solo si $\mathrm{Im}(\alpha) = H$ y $\ker(\alpha) = 1$.

Demostración. (1) Sea α inyectiva y $g \in \ker(\alpha)$. Entonces $\alpha(g) = 1 = \alpha(1)$ y se sigue que $g = 1$.

Recíprocamente, sea $\ker(\alpha) = \{1\}$ y $g, h \in G$ con $\alpha(g) = \alpha(h)$. Entonces $\alpha(g)\alpha(h)^{-1} = 1$ y se sigue que $\alpha(gh^{-1}) = 1$. Esto demuestra que $gh^{-1} \in \ker(\alpha) = \{1\}$, y por tanto, $g = h$.

(2) Se sigue de la definición de epimorfismo.

(3) Es una consecuencia de (1) y (2). □

2.2.8 Ejemplos. (1) Sean V el 4-grupo de Klein y $\alpha : V \longrightarrow V$ definida por $\alpha(x) \coloneqq x^2$. Se verifica que α es un endomorfismo de V, con $\ker(\alpha) = V$.

(2) La función valor absoluto

$$|\cdot| : (\mathbb{C}^\times, \cdot) \longrightarrow (\mathbb{R}^\times, \cdot)$$

define un homomorfismo de grupos cuyo nucleo está dado por

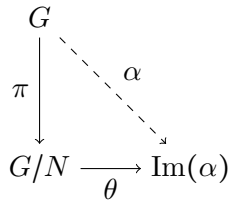
$$\ker(|\cdot|) = S^1 = \{z \in \mathbb{C} \mid |z| = 1\}.$$

2.2.9 Teorema. (Isomorfía 1) Sea G y H grupos.

(1) Si $\alpha \in \mathrm{Hom}(G, H)$, entonces la función $\theta : G/\ker(\alpha) \longrightarrow \mathrm{Im}(\alpha)$ definida por $\theta(g\ker(\alpha)) = \alpha(g)$ es un isomorfismo. Es decir,

$$G/\ker(\alpha) \cong \mathrm{Im}(\alpha). \tag{2.1}$$

(2) Recíprocamente, si $N \trianglelefteq G$, entonces la función $\pi : G \longrightarrow G/N$ definida por $\pi(g) = gN$ es un epimorfismo y $\ker(\pi) = N$. Esta función π la llamamos `epimorfismo canónico`.



Demostración. (1) Del teorema 2.2.6 (6) se tiene que $\ker(\alpha) \trianglelefteq G$.

(a) θ está bien definida: Sean $x, y \in G$.

$$\begin{aligned} x\ker(\alpha) = y\ker(\alpha) &\Leftrightarrow y^{-1}x \in \ker(\alpha) \\ &\Leftrightarrow \alpha(y^{-1}x) = 1 \\ &\Leftrightarrow \alpha(x) = \alpha(y) \\ &\Leftrightarrow \theta(x\ker(\alpha)) = \theta(y\ker(\alpha)) \end{aligned}$$

(b) Es inmediato que θ es un epimorfismo.

(c) θ es un monomorfismo: Sea $x \in G$. Entonces

$$\begin{aligned} x\ker(\alpha) \in \ker(\theta) &\Leftrightarrow \alpha(x) = 1 \\ &\Leftrightarrow x \in \ker(\alpha) \\ &\Leftrightarrow x\ker(\alpha) = \ker(\alpha). \end{aligned}$$

Esto demuestra que $\ker(\theta) = \ker(\alpha) = 1$.

(2) Consideremos la función $\pi : G \longrightarrow G/N$ definida por $\pi(g) = gN$.

(a) π es un homomorfismo: Sean $x, y \in G$. Entonces

$$\pi(xy) = xyN = xN \cdot yN = \pi(x)\pi(y).$$

(b) Claramente π es un epimorfismo.

(c) π es monomorfismo: Sea $x \in G$.

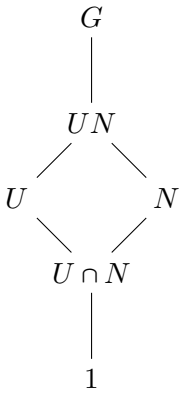
$$x \in \ker(\pi) \Leftrightarrow \pi(x) = 1 \Leftrightarrow xN = N \Leftrightarrow x \in N.$$

Entonces $\ker(\pi) = N$. $\square$

2.2.10 Teorema. (Isomorfía 2) Sean $N \trianglelefteq G$ y $U \leq G$. Entonces

$$UN/N \cong U/(U \cap N).$$

El siguiente gráfico ilustra los subgrupos utilizados en el teorema.



Demostración. Del lema 2.1.9 tenemos que $UN \leq G$ y $U \cap N \trianglelefteq U$. Consideremos la función $\varphi : U \longrightarrow UN/N$ definida por $\varphi(u) := uN$.

(1) Demostramos que φ está bien definida. Sean $u, v \in U$. Si $u = v$, entonces $v^{-1}u = 1 \in N$. Por consiguiente, $v^{-1}uN = N$. Entonces $uN = vN$.

(2) Es inmediato que φ es un epimorfismo.

(3) Sea $u \in U$. Entonces

$$u \in \ker(\varphi) \Leftrightarrow uN = N \Leftrightarrow u \in N \Leftrightarrow u \in U \cap N.$$

Esto demuestra que $\ker(\varphi) = U \cap N$.

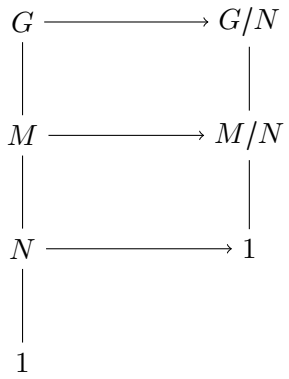
Usando el primer teorema de isomorfía se tiene que

$$U/(U \cap N) = U/\ker(\varphi) \cong \mathrm{Im}(\varphi) = UN/N. \quad \square$$

2.2.11 Teorema. (Isomorfía 3) Sean $N, M \trianglelefteq G$ y $N \leq M$. Entonces $M/N \trianglelefteq G/N$ y además

$$(G/N)/(M/N) \cong G/M.$$

El siguiente gráfico ilustra los subgrupos utilizados en el teorema.



Demostración. Sea $\beta : G/N \longrightarrow G/M$ definida por $\beta(gN) := gM$.

(1) Demostramos que β está bien definida. Sean $g, h \in G$ y supongamos que $gN = hN$. Entonces $h^{-1}g \in N \leq M$. Por lo tanto, que $gM = hM$.

(2) Demostramos que β es un homomorfismo. Sean $g, h \in G$. Entonces

$$\begin{aligned} \beta(gNhN) &= \beta(ghN) \\ &= (gh)M = gMhM \\ &= \beta(gN)\beta(hN). \end{aligned}$$

(3) Es claro que β es un epimorfismo.

(4) Demostramos que β es un monomorfismo. Sea $g \in G$. Entonces

$$gN \in \ker(\beta) \Leftrightarrow gM = M \Leftrightarrow g \in M.$$

Entonces $\ker(\beta) = M/N$ y, por tanto, $M/N \trianglelefteq G/N$. Nuevamente del primer teorema de isomorfía se sigue que

$$(G/N)/(M/N) = (G/N)/\ker(\beta) \cong \mathrm{Im}(\beta) = G/M. \quad \square$$

2.2.12 Teorema. (Cayley) Todo grupo G es isomorfo a un subgrupo de $\mathrm{Sym}(G)$.

Dados dos grupos G y H y un homomorfismo $\alpha : G \longrightarrow H$, en el siguiente teorema establecemos una correspondencia entre los elementos del conjunto de todos los subgrupos de G que contienen a $\ker(\alpha)$ y el conjunto de todos los subgrupos de $\mathrm{Im}(\alpha)$.

2.2.13 Teorema. (Correspondencia) Sea $\alpha \in \mathrm{Hom}(G, H)$. Notemos con $S(G, \ker(\alpha))$ la clase de todos los subgrupos de G que contienen a $\ker(\alpha)$. Esto es,

$$S(G, \ker(\alpha)) = \{U \mid \ker(\alpha) \subseteq U \leq G\}.$$

Notemos además con $S(\mathrm{Im}(\alpha))$ la clase de todos los subgrupos de H contenidos en $\mathrm{Im}(\alpha)$. Esto es, $S(\mathrm{Im}(\alpha)) = \{V \mid V \leq \mathrm{Im}(\alpha)\}$.

Entonces las funciones

$$\tau_1 : S(G, \ker(\alpha)) \longrightarrow S(\mathrm{Im}(\alpha))$$

definida por

$$\tau_1(U) = \alpha(U)$$

y

$$\tau_2 : S(\mathrm{Im}(\alpha)) \longrightarrow S(G, \ker(\alpha))$$

definida por

$$\tau_2(V) = \alpha^{-1}(V)$$

son biyectivas y una es la inversa de la otra.

Demostración. Si $U \in S(G, \ker(\alpha))$, entonces $\tau_1(U) \in S(\mathrm{Im}(\alpha))$ (ver lema 2.2.6).

(1) Demostramos que τ_1 es inyectiva. Sean $U, U' \in S(G, \ker(\alpha))$, para los cuales se verifica que $\tau_1(U) = \tau_1(U')$. Es decir, $\alpha(U) = \alpha(U')$.

Sea $x \in U$. Entonces existe $y \in U'$ tal que $\alpha(x) = \alpha(y)$. En consecuencia, $xy^{-1} \in \ker(\alpha) \subseteq U'$. Por lo tanto, $xy^{-1} \in U'$, y se sigue que $x \in U'$. Esto es, $U \subseteq U'$. Similar se demuestra que $U' \subseteq U$, y se concluye que $U = U'$.

(2) Demostramos que τ_1 es sobreyectiva. Sea $V \in S(\mathrm{Im}(\alpha))$ y definamos $U := \alpha^{-1}(V)$. Del lema 2.2.6 (5) se sigue que $U \leq G$. Si $u \in \ker(\alpha)$, entonces $\alpha(u) = 1 \in V$, con lo cual se tiene que $u \in U$. Esto demuestra que $\ker(\alpha) \subseteq U$. En resumen, se tiene que $\ker(\alpha) \subseteq U \leq G$. Es decir, $U \in S(G, \ker(\alpha))$. Finalmente, note que

$$V = \alpha(\alpha^{-1}(V)) = \alpha(U) = \tau_1(U).$$

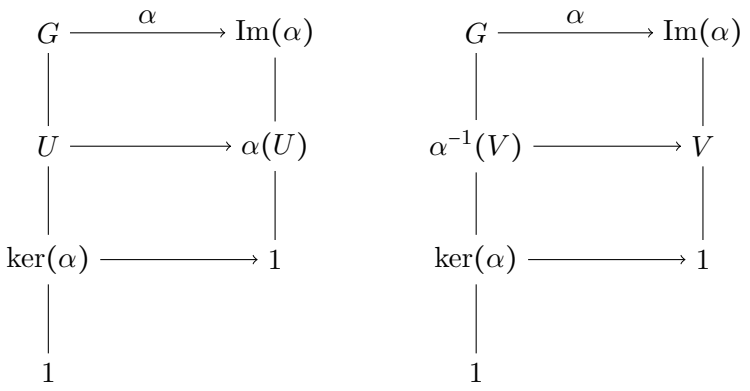
(3) Se deja como ejercicio demostrar que τ_2 es una función biyectiva.

(4) Para probar la ultima afirmación, sea $V \in S(\mathrm{Im}(\alpha))$. Entonces

$$\tau_1(\tau_2(V)) = \tau_1(\alpha^{-1}(V)) = \alpha(\alpha^{-1}(V)) = V.$$

Es decir, $\tau_1 \circ \tau_2 = I_{S(\mathrm{Im}(\alpha))}$. □

El siguiente gráfico ilustra los subgrupos utilizados en el teorema.



2.2.14 Corolario. (Correspondencia) Sea G un grupo, $N \trianglelefteq G$ y $S(G, N)$ la clase $S(G, N) = \{U \mid N \subseteq U \leq G\}$. Notemos con $S(G/N)$ la clase de todos los subgrupos de G/N. Esto es,

$$S(G/N) = \{U/N \mid N \subseteq U \leq G\}.$$

Entonces existe una biyección entre $S(G, N)$ y $S(G/N)$. Además, si $N \subseteq H \trianglelefteq G$, entonces $\tau_1(H) \trianglelefteq G/N$. Finalmente, si $H, H' \in S(G, N)$ con $H \leq H'$, entonces $\tau_1(H) \leq \tau_1(H')$ y $|H' : H| = |\tau_1(H') : \tau_1(H)|$.

DEMOSTRACIÓN. Tomando π como el epimorfismo canónico $\pi(g) = gN$ para todo $g \in G$, la afirmación es una consecuencia del teorema anterior. En efecto, es suficiente definir $\tau_1 : S(G,N) \longrightarrow S(G/N)$ como

$$\tau_1(U) = U/N.$$

Las afirmaciones finales se dejan como ejercicio. □

2.3 Endomorfismos y automorfismos

2.3.1 Lema. Sean $(G,\cdot)$ y $(H,+)$ grupos, con H abeliano. Entonces $\mathrm{Hom}(G,H)$ es un grupo abeliano con respecto a la operación

$$(\alpha+\beta)(g) := \alpha(g)+\beta(g), \quad \alpha,\beta \in \mathrm{Hom}(G,H).$$

DEMOSTRACIÓN. La función $\varepsilon : G \longrightarrow H$, definida por $\varepsilon(g) := 1$ para todo $g \in G$, es un homomorfismo. Por lo tanto, $\mathrm{Hom}(G,H)$ es no vacío y ε es el módulo.

Sean $\alpha,\beta \in \mathrm{Hom}(G,H)$ y $g,h \in G$. Entonces

$$\begin{aligned}(\alpha+\beta)(gh) &= \alpha(gh)+\beta(gh)\\ &= \alpha(g)+\alpha(h)+\beta(g)+\beta(h)\\ &= \alpha(g)+\beta(g)+\alpha(h)+\beta(h)\\ &= (\alpha+\beta)(g)+(\alpha+\beta)(h)\end{aligned}$$

Esto demuestra que $\alpha+\beta \in \mathrm{Hom}(G,H)$. La asociatividad de la operación es evidente. Si definimos $(-\alpha)(g) := -\alpha(g)$, entonces se verifica sin dificultades que $-\alpha \in \mathrm{Hom}(G,H)$ y además es la inversa de α. □

2.3.2 Corolario. El conjunto de los endomorfismos de un grupo abeliano A forma un anillo con elemento identidad.

DEMOSTRACIÓN. Como multiplicación se toma la composición de funciones. □

Note que si G es un grupo, entonces $\mathrm{Aut}(G)$ es un grupo con respecto a la composición de funciones, pero con respecto a la suma definida en el lema anterior en general no lo es. En efecto, si G es un grupo abeliano, entonces las funciones idéntica e inversión son automorfismos de G, no obstante la suma de estas es $\varepsilon \notin \mathrm{Aut}(G)$.

2.3.3 Teorema. Sea G un grupo. Entonces

(1) $\mathrm{Inn}(G) = \{\alpha_g \mid g \in G\} \trianglelefteq \mathrm{Aut}(G)$.

(2) La función $\alpha : G \longrightarrow \mathrm{Inn}(G)$ definida por $\alpha(g) := \alpha_{g^{-1}}$ es un epimorfismo, cuyo núcleo notamos con $Z(G)$ y llamamos el `centro de` G.

(3) Se verifica que

$$Z(G) = \{x \mid x \in G,\ xy = yx, \forall y \in G\}$$

y además $G/Z(G) \cong \mathrm{Inn}(G)$.

Demostración. (1) Dado que $\alpha_1 = \mathrm{I}_G$, se sigue que $\mathrm{Inn}(G) \neq \varnothing$. Sean $\alpha_g, \alpha_h \in \mathrm{Inn}(G)$ y $x \in G$. Entonces

$$\begin{aligned}(\alpha_g\alpha_h)(x) &= \alpha_g(\alpha_h(x)) \\ &= g^{-1}(h^{-1}xh)g \\ &= (hg)^{-1}x(hg) \\ &= \alpha_{hg}(x).\end{aligned}$$

Es decir, $\alpha_g\alpha_h = \alpha_{hg} \in \mathrm{Inn}(G)$. Por otro lado, $\alpha_g\alpha_{g^{-1}} = \alpha_1 = \mathrm{I}_G$, lo cual demuestra que $\alpha_{g^{-1}} = \alpha_g^{-1} \in \mathrm{Inn}(G)$.

Finalmente, sean $\alpha_g \in \mathrm{Inn}(G)$, $\beta \in \mathrm{Aut}(G)$ y $x \in G$. Entonces

$$\begin{aligned}(\beta^{-1}\alpha_g\beta)(x) &= (\beta^{-1}\alpha_g)(\beta(x)) \\ &= \beta^{-1}(g^{-1}\beta(x)g) \\ &= (\beta^{-1}(g))^{-1}x\beta^{-1}(g) \\ &= \alpha_{\beta^{-1}(g)}(x)\end{aligned}$$

Esto demuestra que $\beta^{-1}\alpha_g\beta \in \mathrm{Inn}(G)$ y se tiene la conclusión.

(2) Sean $g, h, x \in G$. Entonces

$$\begin{aligned}\alpha(gh)x &= \alpha_{(gh)^{-1}}(x) \\ &= (gh)x(gh)^{-1} \\ &= ghxh^{-1}g^{-1} \\ &= g(\alpha_{h^{-1}}(x))g^{-1} \\ &= \alpha_{g^{-1}}(\alpha_{h^{-1}}(x)) \\ &= \alpha(g)\alpha(h)x\end{aligned}$$

Esto demuestra que $\alpha(gh) = \alpha(g)\alpha(h)$ para todo $g, h \in G$. Por lo tanto, α es un homomorfismo. Es claro que α es sobreyectiva y, en consecuencia, un epimorfismo.

(3) Determinemos ahora el núcleo de α:

$$\begin{aligned} g \in \ker(\alpha) &\Leftrightarrow \alpha_{g^{-1}} = \mathrm{I}_G \\ &\Leftrightarrow gxg^{-1} = x \text{ para todo } x \in G \\ &\Leftrightarrow gx = xg \text{ para todo } x \in G. \end{aligned}$$

Aplicando ahora el primer teorema de isomorfía se se completa la demostración. □

2.3.4 Observaciones. (1) Un grupo G es abeliano si y solo si $Z(G) = G$.

(2) Si G es abeliano, entonces $\mathrm{Inn}(G) = 1$.

(3) El grupo cociente $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ es denominado el grupo de los `automorfismos exteriores` de G.

(4) $\mathrm{Aut}(G) \leq \mathrm{Sym}(|G|)$ y dado que $\varphi(1) = 1$ para todo $\varphi \in \mathrm{Aut}(G)$, del teorema de Lagrange se sigue que $|\mathrm{Aut}(G)|$ divide a $(|G| - 1)!$

2.3.5 Ejemplo. (Automorfismos del 4-grupo de Klein) Sea $G = \{1, g, h, gh\}$, con $g^2 = h^2 = 1$ y $gh = hg$. De la Observación anterior se sigue que $|\mathrm{Aut}(G)| \in \{1, 2, 3, 6\}$. Definamos

$$\varphi = \begin{pmatrix} 1 & g & h & gh \\ 1 & h & gh & g \end{pmatrix}$$

y

$$\psi = \begin{pmatrix} 1 & g & h & gh \\ 1 & g & gh & h \end{pmatrix}.$$

Entonces

$$\varphi^2 = \begin{pmatrix} 1 & g & h & gh \\ 1 & gh & g & h \end{pmatrix}$$

$$\varphi^3 = \begin{pmatrix} 1 & g & h & gh \\ 1 & g & h & gh \end{pmatrix} = (1)$$

$$\varphi\psi = \begin{pmatrix} 1 & g & h & gh \\ 1 & h & g & gh \end{pmatrix}$$

$$\varphi^2\psi = \begin{pmatrix} 1 & g & h & gh \\ 1 & gh & h & g \end{pmatrix}$$

Se puede verificar que

$$\{(1), \varphi, \psi, \varphi^2, \varphi\psi, \varphi^2\psi\} \subseteq \mathrm{Aut}(G).$$

Por lo tanto,

$$\mathrm{Aut}(G) = \{(1), \varphi, \psi, \varphi^2, \varphi\psi, \varphi^2\psi\}.$$

Se deja como ejercicio demostrar que $\mathrm{Aut}(G) \cong \mathrm{Sym}(3)$. Una consecuencia de este resultado es que el grupo de automorfismos de un grupo abeliano puede no ser conmutativo.

2.4 Conjugación

2.4.1 Definición. Si $x \in G$, entonces el conjunto $\mathrm{ccl}_G(x) := \{x^g \mid g \in G\}$ se denomina `clase de conjugación` de x en G.

2.4.2 Lema. Sea M un subconjunto no vacío de G y $g \in G$ fijo. Entonces M^g es un subgrupo de G si y solo si M lo es.

Demostración. Sean $x, y \in M$. Entonces $x^g(y^g)^{-1} = (g^{-1}xg)(g^{-1}yg)^{-1} = g^{-1}(xy^{-1})g$. Por lo tanto, $x^g(y^g)^{-1} \in M^g \Leftrightarrow xy^{-1} \in M$. □

2.4.3 Lema. Definamos sobre G la siguiente relación: Sea $x, y \in G$.

$$x \sim y \Leftrightarrow \exists g \in G \text{ tal que } x^g = y.$$

Entonces $\sim$ es una relación de equivalencia.

Demostración. Se deja como ejercicio. □

2.4.4 Observación. Las clases de equivalencias de $\sim$ son las clases de conjugación de G. Por lo tanto, se cumple que $G = \bigcup K_i$, donde las K_i denotan las distintas clases de conjugación de G. Si G es finito, entonces $|G| = \sum_{i=1}^{n} |K_i|$. El número n se denomina `número de clases` de G.

2.4.5 Definición. Sea M, X subconjuntos no vacíos de G y $U \leq G$.

(1) El `normalizador` de M en U, notado $N_U(M)$, se define por

$$N_U(M) := \{u \in U \mid M^u = M\} = \{u \in U \mid u^{-1}Mu = M\}.$$

(2) Se dice que X `normaliza a` M si $X \subseteq N_U(M)$.

(3) El `centralizador` de M en U, notado $C_U(M)$, se define de la siguiente manera:

$$C_U(M) = \{u \in U \mid m^u = m,\ \forall m \in M\} = \{u \in U \mid mu = um,\ \forall m \in M\}.$$

Si $M = \{g\}$, entonces escribimos $C_U(g)$ en lugar de $C_U(\{g\})$ y llamamos a $C_U(g)$ el `centralizador` de g en U. Note además que $Z(G) = C_G(G)$.

El siguiente lema nos muestra algunas propiedades del normalizador y del centralizador de un conjunto.

2.4.6 Lema. Sea $\varnothing \neq M \subseteq G$ y $U \leq G$:

(1) $N_U(M)$ y $C_U(M)$ son subgrupos de U.

(2) $C_U(M) \leq N_U(M)$.

(3) $U \leq N_G(U)$.

(4) $Z(G) = \bigcap_{g \in G} C_G(g)$.

Demostración. (1) Dado que $M^1 = M$ y $m^1 = m$ para todo $m \in M$, se tiene que $N_U(M)$ y $C_U(M)$ son conjuntos no vacíos. Sean $x, y \in N_U(M)$. Entonces

$$\begin{aligned} x \in N_U(M) &\Leftrightarrow x^{-1}Mx = M \\ &\Leftrightarrow xMx^{-1} = M \\ &\Leftrightarrow x^{-1} \in N_U(M). \end{aligned}$$

Por lo tanto,

$$M^{xy^{-1}} = (yx^{-1})M(xy^{-1}) = y(x^{-1}Mx)y^{-1} = yMy^{-1} = M.$$

Esto demuestra que $N_U(M) \leq U$.

Sean ahora $x, y \in C_U(M)$ y $m \in M$. Entonces

$$m^{xy^{-1}} = (yx^{-1})m(xy^{-1}) = y(m^x)y^{-1} = ymy^{-1} = m.$$

Esto demuestra que $xy^{-1} \in C_U(M)$ y, por lo tanto, $C_U(M) \leq U$.

(2) Se sigue de la definición.

(3) Sean $x, y \in U$. Entonces se verifica que $U^{xy^{-1}} = U$.

(4) Sea $x \in G$. Entonces

$$\begin{aligned} x \in Z(G) &\Leftrightarrow xg = gx \ \ \forall g \in G \\ &\Leftrightarrow x \in C_G(g) \ \ \forall g \in G \\ &\Leftrightarrow x \in \bigcap_{g \in G} C_G(g) \quad \square \end{aligned}$$

2.4.7 Teorema. Sea M un subconjunto no vacío de G. Entonces el número de conjugados de M en G es igual al número de clases laterales derechas de $N_G(M)$ en G. Es decir,

$$|\{M^g \mid g \in G\}| = |G : N_G(M)|.$$

Demostración. Sean $g, h \in G$. Entonces

$$\begin{aligned} g^{-1}Mg = h^{-1}Mh &\Leftrightarrow (hg^{-1})M(gh^{-1}) = M \\ &\Leftrightarrow gh^{-1} \in N_G(M) \\ &\Leftrightarrow N_G(M)g = N_G(M)h. \end{aligned}$$

En conclusión, $N_G(M)$ tiene tantas clases laterales derechas distintas en G como conjugados distintos tenga M. $\square$

2.4.8 Lema. Sean $\varnothing \neq M \subseteq G$ y $U \leq G$. Entonces

(1) $U \trianglelefteq G$ si y solo si $N_G(U) = G$.

(2) $U \trianglelefteq N_G(U)$ y todo subgrupo de G en el cual U es normal está contenido en $N_G(U)$. Es decir, $N_G(U)$ es el subgrupo más grande de G en el cual U es normal.

Demostración. Se deja como ejercicio. $\square$

2.4.9 Teorema. Sea $U \leq G$. Entonces $C_G(U) \trianglelefteq N_G(U)$, y además $N_G(U)/C_G(U)$ es isomorfo a un subgrupo de $\mathrm{Aut}(U)$.

Demostración. Consideremos nuevamente la función α del teorema 2.3.3, restringida a $N_G(U)$. Esto es, $\alpha : N_G(U) \longrightarrow \mathrm{Aut}(U)$ definida por $\alpha(x) := \alpha_{x^{-1}}$. Se verifica que α es un homomorfismo, cuyo núcleo es $C_G(U)$. La conclusión se obtiene del primer teorema de isomorfía. $\square$

2.4.10 Definición. (1) Un subgrupo U de G se denomina `característico` si $\alpha(U) \subseteq U$ para todo $\alpha \in \mathrm{Aut}(G)$. Esto lo simbolizamos con U char G.

(2) U se llama `completamente invariante` si $\alpha(U) \subseteq U$ para todo $\alpha \in \mathrm{End}(G)$.

2.4.11 Observación. Si U char G, entonces $\alpha(U) = U$ para todo $\alpha \in \mathrm{Aut}(G)$. En efecto para todo $\alpha \in \mathrm{Aut}(G)$ se sigue $\alpha^{-1}(U) \subseteq U$. Por lo tanto, $U \subseteq \alpha(U)$ para todo $\alpha \in \mathrm{Aut}(G)$.

2.4.12 Lema. Sean $U, V, N \leq G$.

(1) Si U es un subgrupo completamente invariante, entonces U char G.

(2) Si N char G, entonces $N \trianglelefteq G$.

(3) Las relaciones `ser subgrupo característico` y `ser subgrupo completamente invariante` son transitivas.

(4) Si U char N y $N \trianglelefteq G$, entonces $U \trianglelefteq G$.

(5) Si $U \leq V \leq G$ con U char G y V/U char G/U, entonces V char G.

Demostración. (1) Se sigue del hecho que $\mathrm{Aut}(G) \subseteq \mathrm{End}(G)$.

(2) Se sigue del hecho que $\mathrm{Inn}(G) \subseteq \mathrm{Aut}(G)$.

(3) Supongamos que U char V y V char G y sea $\alpha \in \mathrm{Aut}(G)$. Entonces $\alpha(V) \subseteq V$, y además α induce un automorfismo sobre V que deja invariante a U. Entonces $\alpha(U) \subseteq U$, y se demuestra que U char G. Un razonamiento similar demuestra el caso `completamente invariante`. Note que la restricción de un endomorfismo (automorfismo) a un subgrupo completamente invariante (característico) es un endomorfismo (automorfismo).

(4) Sea $\alpha_g \in \mathrm{Inn}(G)$. Dado que $N \trianglelefteq G$, se tiene que $\alpha_g(N) = N$. Si definimos $\widetilde{\alpha}_g$ como la restricción de α_g a N, entonces $\widetilde{\alpha}_g \in \mathrm{Aut}(N)$ y se verifica que $\alpha_g(U) = U$. Por lo tanto, $U \trianglelefteq G$.

(5) Se deja como ejercicio. □

2.4.13 Observación. Es evidente que la relación $\leq$ es transitiva, sin embargo, la normalidad no es una relación transitiva. Es decir, si $U \trianglelefteq N$ y $N \trianglelefteq G$, no necesariamente $U \trianglelefteq G$. Por ejemplo, considere el grupo alternante de grado 4 y sus subgrupos $U = \langle (12)(34) \rangle$ y $V_4 = \{(1), (12)(34), (13)(24), (14)(23)\}$. Se verifica que $U \trianglelefteq V_4$ y $V_4 \trianglelefteq \mathrm{Alt}(4)$, sin embargo $U \not\trianglelefteq \mathrm{Alt}(4)$.

2.4.14 Ejemplos. (1) El centro de un grupo G es característico. Sea $x \in Z(G)$, $g \in G$ y $\alpha \in \mathrm{Aut}(G)$. Entonces $\alpha(x)g = \alpha(x)\alpha(h)$ para algún $h \in G$. Por lo tanto, $\alpha(x)g = \alpha(xh) = \alpha(hx) = \alpha(h)\alpha(x) = g\alpha(x)$. Esto demuestra que $\alpha(x)$ conmuta con cada elemento de G. Se deja como ejercicio verificar que $Z(G)$ no es un subgrupo completamente invariante.

(2) Sea $U \leq G$. Si U es el único subgrupo de G con orden n, entonces U char G. Sea $\alpha \in \mathrm{Aut}(G)$. Entonces $|\alpha(U)| = |U| = n$. Por otro lado, $\alpha(U) \leq G$, y dado que U es único subgrupo de G con orden n, se tiene que $\alpha(U) = U$.

Como ilustración, considere el grupo $\mathrm{Sym}(3)$ y $U = \langle (123) \rangle$. Recuerde que U es el único subgrupo de orden 3 en $\mathrm{Sym}(3)$. Por lo tanto, U char $\mathrm{Sym}(3)$.

(3) Si $k \in \mathbb{N}$ y definimos $G^k := \langle g^k \mid g \in G \rangle$, entonces G^k es un subgrupo completamente invariante de G. En efecto, si $x \in G^k$, entonces $x = x_1^{\epsilon_1} \cdots x_n^{\epsilon_n}$, donde $n \in \mathbb{N}$, $x_i = g_i^k$ y $g_i \in G$. Sea ahora $\alpha \in \mathrm{End}(G)$. Entonces

$$\alpha(x) = \alpha(x_1)^{\epsilon_1} \cdots \alpha(x_n)^{\epsilon_n} = \alpha(g_1)^{k\epsilon_1} \cdots \alpha(g_n)^{k\epsilon_n} = (h_1^k)^{\epsilon_1} \cdots (h_n^k)^{\epsilon_n} \in G^k.$$

Como ilustración, consideremos nuevamente el grupo $\mathrm{Sym}(3)$. Note que

$$\mathrm{Sym}(3)^2 = \langle g^2 \mid g \in G \rangle = \langle (123) \rangle \quad \text{y} \quad \mathrm{Sym}(3)^3 = \langle g^3 \mid g \in G \rangle = \mathrm{Sym}(3).$$

2.4.15 Teorema. Sean $M, N \trianglelefteq G$, con $M \leq N$. Sea $\mathcal{A}$ un subgrupo de $\mathrm{Aut}(G)$ y supongamos que para todo $\alpha \in \mathcal{A}$ se cumple que $\alpha(M) = M$ y $\alpha(N) = N$. Entonces la función $\widetilde{\alpha} : N/M \longrightarrow N/M$ definida por $\widetilde{\alpha}(nM) = \alpha(n)M$ para todo $n \in N$, es un automorfismo de N/M. La función $\mu : \mathcal{A} \longrightarrow \mathrm{Aut}(M/N)$ definida por $\mu(\alpha) := \widetilde{\alpha}$ es un homomorfismo. Además, $\ker(\mu)$ consta de todos los automorfismos $\alpha \in \mathcal{A}$ que tienen la forma $\alpha(n) = nm(n)$, con $m(n) \in M$ para todo $n \in N$.

Demostración. (1) Demostramos inicialmente que $\widetilde{\alpha}$ está bien definida. Sean $n_1, n_2 \in N$ y supongamos que $n_1 M = n_2 M$. Entonces $n_2^{-1} n_1 \in M$. Es decir, $n_1 = n_2 m$ para algún $m \in M$. En consecuencia, dado que $\alpha(m) \in M$, se tiene que

$$\widetilde{\alpha}(n_1 M) = \alpha(n_1)M = \alpha(n_2)\alpha(m)M = \alpha(n_2)M = \widetilde{\alpha}(n_2 M).$$

(2) Demostramos que $\widetilde{\alpha}_g$ es un homomorfismo. Sean $n_1, n_2 \in N$. Entonces

$$\begin{aligned} \widetilde{\alpha}(n_1 M n_2 M) &= \widetilde{\alpha}(n_1 n_2 M) \\ &= \alpha(n_1 n_2)M \\ &= \alpha(n_1)\alpha(n_2)M \\ &= \alpha(n_1)M\alpha(n_2)M \\ &= \widetilde{\alpha}(n_1 M)\widetilde{\alpha}(n_2 M). \end{aligned}$$

(3) Es claro que $\widetilde{\alpha}$ es invertible y, por lo tanto, $\widetilde{\alpha} \in \mathrm{Aut}(H/K)$.

(4) Demostramos que μ es un homomorfismo. Sean $\alpha_1, \alpha_2 \in \mathcal{A}$. Entonces para todo $n \in N$ tenemos que

$$\begin{aligned}\mu(\alpha_1\alpha_2)(nM) &= \widetilde{\alpha_1\alpha_2}(nM) \\ &= \alpha_1\alpha_2(n)M \\ &= \alpha_1(\alpha_2(n))M \\ &= \widetilde{\alpha_1}(\alpha_2(n)M) \\ &= \widetilde{\alpha_1}(\widetilde{\alpha_2}(nM)) \\ &= \widetilde{\alpha_1}\widetilde{\alpha_2}(nM) \\ &= \mu(\alpha_1)\mu(\alpha_2)(nM).\end{aligned}$$

Con esto se tiene la afirmación.

(5) Finalmente, calculemos $\ker(\mu)$.

$$\begin{aligned}\ker(\mu) &= \{\alpha \in \mathcal{A} \mid \widetilde{\alpha} = \mathrm{I}_{M/N}\} \\ &= \{\alpha \in \mathcal{A} \mid \widetilde{\alpha}(nM) = nM,\ \forall n \in N\} \\ &= \{\alpha \in \mathcal{A} \mid \alpha(n)M = nM,\ \forall n \in N\} \\ &= \{\alpha \in \mathcal{A} \mid n^{-1}\alpha(n) \in M,\ \forall n \in N\} \\ &= \{\alpha \in \mathcal{A} \mid \alpha(n) = nm(n),\ m(n) \in M, \forall n \in N\}. \quad \square\end{aligned}$$

2.4.16 Observación. Consideremos un caso especial del teorema anterior. Por ejemplo, sea $\mathcal{A} = \mathrm{Inn}(G)$. Esto es, para $\alpha_g \in \mathrm{Inn}(G)$ definamos la función $\widetilde{\alpha}_g : N/M \longrightarrow N/M$ de la siguiente manera:

$$\widetilde{\alpha}_g(nM) = \alpha_g(n)M = n^g M.$$

Sea además $\theta : G \longrightarrow \mathrm{Aut}(H/K)$ definida por

$$\theta(g) := \widetilde{\alpha}_{g^{-1}}.$$

Se verifica que θ es un homomorfismo. Para demostrarlo, sean $g_1, g_2 \in G$. Entonces

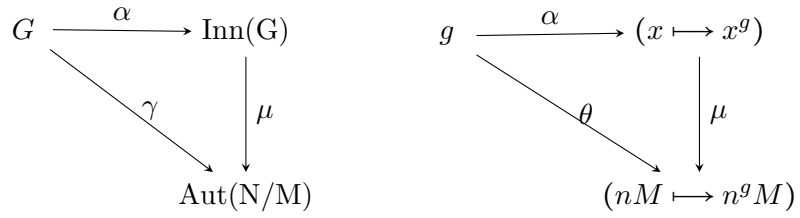
$$\theta(g_1g_2) = \widetilde{\alpha}_{(g_1g_2)^{-1}} = \widetilde{\alpha}_{g_2^{-1}g_1^{-1}} = \widetilde{\alpha}_{g_1^{-1}}\widetilde{\alpha}_{g_2^{-1}} = \theta(g_1)\theta(g_2).$$

El núcleo de θ es notado con $C_G(H/K)$ y está dado por

$$\begin{aligned}\ker(\theta) &= \{g \in G \mid \widetilde{\alpha}_{g^{-1}} = \mathrm{I}_{N/M}\} \\ &= \{g \in G \mid \widetilde{\alpha}_{g^{-1}}(nM) = nM,\ \forall n \in N\} \\ &= \{g \in G \mid n^{g^{-1}}M = nM,\ \forall n \in N\}.\end{aligned}$$

Como consecuencia del primer teorema de isomorfía se tiene que $G/C_G(H/K)$ es isomorfo a un subgrupo de $\mathrm{Aut}(H/K)$, el cual es notado con $\mathrm{Aut}_G(N/M)$.

En el siguiente diagrama ilustramos los homomorfismos determinados por el teorema y la observación anterior.



2.5 Ejercicios

1. Sea $\{N_j\}_{j\in \mathrm{J}}$ una familia de subgrupos normales de G. Definamos

$$I := \bigcap\{N_j \mid j \in J\} \text{ y } \quad T := \langle N_j \mid j \in J\rangle.$$

   Demuestre que $I, T \trianglelefteq G$.

2. Sea $G = \mathrm{GL}_2(\mathbb{R})$ con la multiplicación usual de matrices y

$$N = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \;\middle|\; a \in \mathbb{R}^\times \right\}.$$

   Verifique que $N \trianglelefteq G$ y además $|G : N| = 2$.

3. Para cada uno de los grupos $\mathrm{Sym}(3), \mathbb{Q}_8, D_8$ y $\mathrm{Alt}(4)$ determine:

   (a) todos sus subgrupos normales,

   (b) los normalizadores de sus subgrupos,

   (c) su centro,

   (d) sus automorfismos interiores.

4. Demuestre que D_8 no es isomorfo a $\mathbb{Q}_8$.

5. Sean

$$G = \left\{ \begin{pmatrix} m & b \\ 0 & 1 \end{pmatrix} \;\middle|\; m \in \mathbb{R}^\times,\ b \in \mathbb{R} \right\} \leq \mathrm{GL}_2(\mathbb{R})$$

y

$$N = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \;\middle|\; b \in \mathbb{R} \right\}$$

Demuestre que G es un grupo con la multiplicación usual de matrices, $N \trianglelefteq G$ y $G/N \cong (\mathbb{R}^\times, \cdot)$.

6. Sea $(G, \cdot)$ un grupo y $H := \mathrm{End}(G)$. Si definimos para $\alpha, \beta \in H$ la operación

$$(\alpha * \beta)(g) := \alpha(g) \cdot \beta(g), \quad \forall \ g \in G$$

   (a) ¿Es $(H, *)$ un grupo?

   (b) ¿Lo es con la composición de funciones?

7. Encuentre un grupo G y subgrupos H, J, K de G tales que $H \trianglelefteq J$, $J \trianglelefteq K$ y sin embargo $H \ntrianglelefteq G$.

8. Sea G un grupo. Demuestre que si $G/Z(G)$ es cíclico, entonces G es abeliano.

9. Sea G un grupo finito. Demuestre que

   (a) Si $U < G$, entonces $G \neq UU^x$ para todo $x \in G$.

   (b) Si p es el número primo más pequeño que divide a $|G|$ y N es un subgrupo de G con $|G : N| = p$, entonces $N \trianglelefteq G$.

   (c) Si $|G| = p^2$ con p un número primo, entonces G es abeliano.

10. Considere la función $\varphi : \mathbb{Z}_4 \times \mathbb{Z}_6 \longrightarrow \mathbb{Z}_4 \times \mathbb{Z}_3$ definida por

$$\varphi(x, y) = (x + 2y, y).$$

    (a) Demuestre que φ está bien definida y es un homomorfismo de grupos.

    (b) Halle el núcleo y la imagen de φ.

    (c) Aplicando el primer teorema de isomorfía, ¿qué puede concluir?

11. Halle el conjunto de todos los automorfismos interiores de un grupo abeliano G.

12. Sea $(\mathbb{Z}, +)$ y $g = 3$. Halle el automorfismo interior α_g.

13. Sea $m \in \mathbb{Z}$ y G un grupo y defina $\varphi_m : G \longrightarrow G$ mediante

$$\varphi_m(g) = g^m.$$

    Demuestre que si G es abeliano, entonces φ_m es un homomorfismo.

14. Para cada uno de los grupos $\mathrm{GL}_2(2)$, $\mathrm{Sym}(3), \mathbb{Q}_8, D_8$ y $\mathrm{Alt}(4)$ determine:

(a) su subgrupos normales

(b) los normalizadores en G de cada subgrupo

(c) los centralizadores en G de cada subgrupo

(d) el centro

(e) las clases de conjugación

(f) los automorfismos interiores.

15. Demuestre que D_8 no es isomorfo a $\mathbb{Q}_8$.

16. Para $n \in \mathbb{N}$ determine $|\mathrm{GL}_2(n) : \mathrm{SL}_2(n)|$.

17. ¿Cuántos elementos tienen los grupos $\mathrm{GL}_2(3)$ y $\mathrm{SL}_2(3)$?

18. Determine $Z(\mathrm{GL}_2(2))$ y $Z(\mathrm{Sym}(3)) = 1$.

19. Determine $\mathrm{Aut}(\mathrm{Sym}(3))$ y demuestre que $\mathrm{Sym}(3) \cong \mathrm{Inn}(\mathrm{Sym}(3))$.

20. ¿Existen grupos no isomorfos con grupos de automorfismos isomorfos?

21. Sea N un subgrupo normal de un grupo G y sean $A, B \leq G$ tales que $A \trianglelefteq B$. Demuestre que $NA \trianglelefteq NB$.

22. Sea $\varphi \in \mathrm{Hom}(G, H)$ y X un sistema de generadores del grupo G. Demuestre que φ queda determinado de manera única por las imágenes de los elementos de X.

23. Muestre un grupo G para el cual no se cumpla que $Z(G)$ es un subgrupo completamente invariante.

24. Sea G un grupo. Demuestre que G es abeliano si se cumple alguna de las siguientes afirmaciones:

(a) $x \longmapsto x^{-1}$ es un endomorfismo de G.

(b) $x \longmapsto x^2$ es un endomorfismo de G.

(c) $x^2 = 1$ para todo $x \in G$.

25. Un grupo G se denomina `metaabeliano` si admite un subgrupo normal N cuyo grupo factor G/N es abeliano. Demuestre o refute: todo subgrupo de un grupo metaabeliano es también es metaabeliano.

26. Demuestre que el grupo de automorfismos del 4-grupo de Klein es isomorfo a $\mathrm{Sym}(3)$.

27. Muestre un ejemplo de un subgrupo que sea normal en un grupo y que no sea un subgrupo característico.

28. Sea G un grupo y $H \leq G$. Suponga que $g^2 \in H$ para todo $g \in G$. Demuestre que $H \trianglelefteq G$ y G/H es abeliano.

29. Sea $\varphi \in \mathrm{Hom}(G, H)$. Demuestre que

    (a) Si $N \trianglelefteq H$, entonces $\varphi^{-1}(N) = \{g \in G \mid \varphi(g) \in N\} \trianglelefteq G$.

    (b) Si $N \trianglelefteq G$ y φ es un epimorfismo, entonces $\varphi(N) \trianglelefteq H$.

30. Sea G un grupo y $N \trianglelefteq G$ con $|G : N| = k$. Demuestre que

    (a) Si $g \in G$, entonces $g^k \in N$.

    (b) Si $\mathrm{mcd}(m, k) = 1$ y $g \in G$ con $g^m \in N$, entonces $g \in N$.

31. Complete la prueba del lema 2.4.8.

32. Complete la prueba del lema 2.4.12.

33. Determine el número de monomorfismos de $(\mathbb{Z}_6, +)$ en $(\mathrm{Sym}(5), \circ)$.

34. Exiba un grupo $G \neq 1$ con $\mathrm{Aut}(G) = 1$.

35. Sea G un grupo finito con orden n. Demuestre que $\mathrm{Aut}(G)$ es un grupo finito y además $|\mathrm{Aut}(G)|$ divide a $(n-1)!$

36. Sea G un grupo. Demuestre que

    (a) Si $H \leq K \leq G$, entonces $N_K(H) = N_G(H) \cap K$.

    (b) $N_G(M)^g = N_G(M^g)$ para todo $\varnothing \neq M \subseteq G$ y todo $g \in G$.

    (c) $C_G(M)^g = C_G(M^g)$ para todo $\varnothing \neq M \subseteq G$ y todo $g \in G$.

37. Sean $\varphi \in \mathrm{Hom}(A, B)$, C y G grupos. Demuestre que

    (a) φ induce una función

    $$\varphi_G : \mathrm{Hom}(G, A) \longrightarrow \mathrm{Hom}(G, B)$$

    mediante $\varphi_G(\alpha) = \varphi \circ \alpha$.

    (b) φ induce una función

    $$\varphi^G : \mathrm{Hom}(B, G) \longrightarrow \mathrm{Hom}(A, G)$$

    mediante $\varphi^G(\alpha) = \alpha \circ \varphi$.

    (c) Si $\psi \in \mathrm{Hom}(B, C)$, entonces

    $$(\psi \circ \varphi)_G = \psi_G \circ \varphi_G \quad \text{y} \quad (\psi \circ \varphi)^G = \varphi^G \circ \psi^G.$$

(d) $(I_G)_G = I_{\mathrm{End}(G)}$ y $(I_G)^G = I_{\mathrm{End}(G)}$.

38. Sea G un grupo y $H \leq G$, con $|G : H| = n$. Sea $G = \bigcup_{i=1}^{n} Hg_i$ una unión disyunta y definamos $\Omega := \{Hg_1, \ldots, Hg_n\}$. Demuestre que

    (a) La función $\alpha : G \longrightarrow \mathrm{Sym}(\Omega)$ definida por

    $$g \longmapsto (Hg_i \longmapsto Hg_ig)$$

    es un homomorfismo.

    (b) $\ker(\alpha) = \bigcap_{i=1}^{n} H^{g_i} = \bigcap_{g\in G} H^g$.

39. Sea V un espacio vectorial sobre un cuerpo K y $B = (v_1, \ldots, v_n)$ una base para V. Demuestre que

    (a) El conjunto de todos los endomorfismos $A \in \mathrm{Hom}(V)$ con

    $$A(v_j) := \sum_{i=1}^{j} a_{ij}v_i, \quad a_{jj} \neq 0, \quad (j = 1, \ldots, n)$$

    forma un subgrupo $\mathcal{U}$ del grupo $\mathrm{GL}(V)$.

    (b) El subconjunto $\mathcal{N}$ de todos los elementos de $\mathcal{U}$ con $a_{ii} = 1$, para $i = 1, \ldots, n$ es un subgrupo normal de $\mathcal{U}$ y además $\mathcal{U}/\mathcal{N}$ es abeliano.

40. Sea G un grupo y $g \in G$.

    (a) Definamos $\psi_g : G \longrightarrow G$ por $\psi_g(x) := gx$ para todo $x \in G$. Demuestre que ψ_g es una biyección.

    (b) Si $h \in G$, demuestre que $\psi_g \circ \psi_h = \psi_{gh}$.

    (c) Sea $\mathrm{Sym}(G) := \{f : G \longrightarrow G \mid f \text{ es biyectiva}\}$ y definamos $\psi : G \longrightarrow \mathrm{Sym}(G)$ por $\psi(g) := \psi_g$ para todo $g \in G$. Demuestre que ψ es un homomorfismo.

41. Sea $\varphi : (\mathbb{R}, +) \longrightarrow (\mathbb{C}, \cdot)$ definida por $\varphi(x) = \cos(2\pi x) + i\sin(2\pi x)$. Demuestre que φ es un homomorfismo y use el primer teorema de isomorfía para probar que $\mathbb{R}/\mathbb{Z} \cong S^1$.

42. Sean $m, n \in \mathbb{N}$. Describa el conjunto $\mathrm{Hom}(\mathbb{Z}_n, \mathbb{Z}_m)$.

43. Sea V un espacio vectorial de dimensión 2 sobre $\mathbb{Z}_3$. Se verifica que V admite cuatro subespacios vectoriales de dimensión 1. Demuestre que existe un epimorfismo de $\mathrm{GL}_2(3)$ en $\mathrm{Sym}(4)$.

44. Sea G un grupo finito y $\alpha \in \mathrm{Aut}(G)$. Demuestre que

    (a) Si $\alpha^2 = I_G$ y $\alpha(x) \neq x$ para todo $x \in G \setminus 1$, entonces G es abeliano y $|G|$ es un número impar.

(b) El conjunto
$$C_G(\alpha) := \{g \in G \mid \alpha(g) = g\}$$
es un subgrupo de G.

(c) Si $\alpha^2 = I_G$ y $|G|$ es un número impar, entonces toda clase lateral de $C_G(\alpha)$ en G contiene un único $g \in G$ con $\alpha(g) = g^{-1}$.

45. Sea G un grupo abeliano y notemos con $\mathrm{Ch}(G)$ el conjunto de todos los homomorfismos de G en el grupo multiplicativo de los números complejos $\mathbb{C}^\times$. Defina en $\mathrm{Ch}(G)$ la siguiente multiplicación:
$$\chi_1\chi_2(x) = \chi_1(x)\chi_2(x).$$
Demuestre que

(a) $\mathrm{Ch}(G)$ es un grupo con la anterior multiplicación.

(b) $\mathrm{Ch}(G) \cong G$.

46. `Definición.` Sea (X, τ) un espacio topológico. Si existe una métrica d definida sobre X que induce la topología τ, entonces (X, τ) se denomina metrizable.

`Definición.` Sea (H, d_H) un grupo abeliano metrizable. Se dice que d_H es una métrica de grupo si se verifica
$$d_H(xy, zw) = d_H(x, z) + d_H(y, w).$$
Sea G y H grupos metrizables y H es abeliano y d_H es una métrica de grupo. Si definimos
$$\widetilde{d}(\varphi, \psi) := \sup_{1 \neq t \in G} \left\{ \frac{d_H(\varphi(t), \psi(t))}{d_G(t, 1) + d_H(\varphi(t), \psi(t))} \right\}.$$
Demuestre que

(a) $(\mathrm{Hom}(G, H), \widetilde{d})$ es un espacio métrico.

(b) $\widetilde{d}$ es una métrica de grupo.

47. Sea $\mathcal{M} := \{U_j \mid j \in \mathrm{J}\}$ un conjunto de subgrupos del grupo G, el cual es cerrado bajo intersecciones finitas y uniones arbitrarias. Sea $\mathcal{O}^*$ el conjunto de las clases laterales derechas de subgrupos de $\mathcal{M}$. Esto es, $\mathcal{O}^* = \{U_j g \mid j \in \mathrm{J},\ g \in G\}$. Definamos $\mathcal{O} := \mathcal{O}^* \cup \varnothing \cup G$. Demuestre:

(a) $\mathcal{O}$ es una topología para G. Es decir, el grupo G se convierte en un espacio topológico y las clases laterales derechas de los U_j forman las vecindades abiertas en G.

(b) Si $\bigcap_{j \in \mathrm{J}} U_j = \langle 1 \rangle$, entonces G con respecto a $\mathcal{O}$ es un espacio de Hausdorff.

(c) Si todo los subgrupos U_j, $j \in \mathrm{J}$ tienen índice finito en G, entonces G es un espacio topológico compacto.

CAPÍTULO 3

GRUPO SIMÉTRICO Y GRUPO ALTERNANTE

> Se parte de uno o varios temas y se les somete a transformaciones geométricas que mantienen la forma del tema: traslaciones, giros y simetrías que confieren a la obra una estructura muy rígida, pero en la que el compositor (Johann Sebastian Bach) encontró una fuente de inspiración.
>
> (El arte de la fuga - 1751)

Uno de los principales resultados de este capítulo es demostrar que existe un único homomorfismo (no trivial) de $\mathrm{Sym}(n)$ en el grupo multiplicativo de un cuerpo K. Este resultado trae como consecuencia que $\mathrm{Sym}(n)$ admite un subgrupo normal de índice 2, el denominado `grupo alternate` de grado n.

A lo largo del capítulo Ω denota el conjunto de los primeros n números enteros positivos. Es decir, $\Omega = \{1, \ldots, n\}$.

3.1 La notación de ciclos

3.1.1 Definición. Sea $k \in \mathbb{N}$.

(1) $\pi \in \mathrm{Sym}(n)$ se denomina un k-ciclo si existe $A = \{a_1, \ldots, a_k\} \subseteq \Omega$ tal que $\pi(a_1) = a_2$, $\pi(a_2) = a_3$, …, $\pi(a_{k-1}) = a_k$, $\pi(a_k) = a_1$ y $\pi(x) = x$ para todo $x \in \Omega \setminus A$. Para abreviar

utilizamos la notación

$$\pi = (a_1\ a_2 \dots a_k).$$

Note que los k-ciclos $(a_1\ a_2 \dots a_k)$ y $(a_k\ a_1 \dots a_{k-1})$ representan la misma permutación.

(2) Un 2-ciclo se denomina una transposición. Es decir, una transposición intercambia dos números y deja fijo al resto. Evidentemente, si π es una transposición, entonces $\pi^2 = \mathrm{I}_\Omega$ y $\pi^{-1} = \pi$.

3.1.2 Teorema. $\mathrm{Sym}(n)$ tiene $n!$ elementos. Esto es, $|\mathrm{Sym}(n)| = n!$

Demostración. Sea $\Omega = \{1, \dots, n\}$. En primer lugar es importante anotar lo siguiente: dado que $\pi \in \mathrm{Sym}(n)$ es una biyección, debe cumplirse que $\pi(i) \neq \pi(j)$ para todo $i, j \in \Omega$, con $i \neq j$. Entonces para $\pi(1)$ existen n posibilidades.

$\pi(2)$ puede ser cualquiera de los números del 1 al n, exceptuando $\pi(1)$, es decir, tenemos $n-1$ posibilidades para $\pi(2)$. En total tenemos $n(n-1)$ posibilidades para dejar fijos a $\pi(1)$ y $\pi(2)$.

En general, para la elección de $\pi(j)$ tenemos $n-(j-1)$ posibilidades, ya que $\pi(j) \notin \{\pi(1), \pi(2), \cdots, \pi(j-1)\}$. Entonces se sigue que el número de elementos de $\mathrm{Sym}(n)$, el cual notamos con $|\mathrm{Sym}(n)|$, está dado por

$$|\mathrm{Sym}(n)| = \prod_{j=1}^{n}(n-j+1) = n(n-1)\cdots 3 \cdot 2 \cdot 1 = n! \qquad \square$$

Consideramos a $\mathrm{Sym}(n)$ como un grupo usando la composición de funciones como operación binaria. Si $\sigma \in \mathrm{Sym}(n)$ y $m \in \mathbb{N}$, entonces escribimos σ^m para denotar la composición de σ con si mismo m-veces.

3.1.3 Definición. Sean $\sigma = (a_{i_1}, \dots, a_{i_k})$ y $\pi = (b_{i_1}, \dots, b_{i_m})$ elementos de $\mathrm{Sym}(n)$. Decimos que σ y π son disjuntos si

$$\{a_{i_1}, \dots, a_{i_k}\} \cap \{b_{i_1}, \dots, b_{i_m}\} = \varnothing.$$

En el siguiente teorema se demuestra que toda permutación de $\mathrm{Sym}(n)$ puede expresarse como un producto de ciclos disjuntos.

3.1.4 Teorema. (1) Todo $\sigma \in \mathrm{Sym}(n)$ tiene una descomposición en ciclos de la forma

$$\sigma = (a_1\sigma(a_1) \dots \sigma^{n_1-1}(a_1)) \cdots (a_k\sigma(a_k) \dots \sigma^{n_k-1}(a_k)),$$

donde $n_j \in \mathbb{N}$, $\sum_{j=1}^{k} n_j = n$ y

$$\Omega = \bigcup_{j=1}^{n} \{a_j, \sigma(a_j) \ldots, \sigma^{n_j-1}(a_j)\}.$$

(2) Se verifica además que

$$(a_1 a_2 \ldots a_k) = (a_1 a_k)(a_1 a_{k-1}) \cdots (a_1 a_2).$$

Esto es, toda permutación es un producto de transposiciones.

DEMOSTRACIÓN. (1) Comenzamos con $a_1 = 1$ y consideremos los números $\sigma^{j-1}(a_1)$, con $j \in \mathbb{N}$. Dado que Ω es un conjunto finito, estos números no son todos distintos. Es decir, existe $n_1 \in \mathbb{N}$ tal que

$$a_1, \sigma(a_1), \ldots, \sigma^{n_1-1}(a_1)$$

son distintos, y además se verifica que

$$\sigma^{n_1}(a_1) \in \{a_1, \sigma(a_1), \ldots, \sigma^{n_1-1}(a_1)\}.$$

Esto es, existe k con $0 \leq k < n_1$ y $\sigma^{n_1}(a_1) = \sigma^k(a_1)$. Entonces $\sigma^{n_1-k}(a_1) = a_1$. Por la elección de n_1 se sigue que $k = 0$ y se tiene que $\sigma^{n_1-1}(a_1) = a_1$.

Si $n_1 < n$, elegimos $a_2 \in \Omega \setminus \{a_1, \sigma(a_1), \ldots, \sigma^{n_1-1}(a_1)\}$. Entonces

$$\{\sigma^j(a_1) \mid j \in \mathbb{N}\} \cap \{\sigma^j(a_2) \mid j \in \mathbb{N}\} = \varnothing$$

y tenemos un nuevo ciclo

$$(a_2 \sigma(a_2) \ldots \sigma^{n_2-1}(a_2)).$$

Después de un número finito de pasos se tiene la afirmación.

(2) Si $x_j \in \Omega \setminus \{a_1, \ldots, a_k\}$, entonces el ciclo $(a_1 \ldots a_k)$ deja fijo a x_j. Por otro lado, si $j = k$, se verifica que

$$(a_1 a_k)(a_1 a_{k-1}) \cdots (a_1 a_2)(a_j) = a_1$$

y si $j < k$, entonces se tiene que

$$(a_1 a_k)(a_1 a_{k-1}) \cdots (a_1 a_2)(a_j) = (a_1 a_k) \cdots (a_1 a_{j+1})(a_j) = a_{j+1}$$

y se tiene la afirmación. □

3.1.5 Ejemplo. Consideremos la permutación

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 4 & 2 & 5 & 7 & 6 \end{pmatrix} \in \mathrm{Sym}(7)$$

La descomposición de σ en ciclos y transposiciones está dada por

$$\sigma = (67)(5)(1342) = (67)(12)(14)(13)$$

3.2 El signo de una permutación

3.2.1 Definición. Sea $\mathcal{T}$ el conjunto definido por

$$\mathcal{T} := \{\{i,j\} \mid i,j \in \Omega, \text{ con } i<j\}.$$

Para $t \in \mathcal{T}$ y $\sigma \in \mathrm{Sym}(n)$ definimos

$$\zeta_\sigma(t) := \begin{cases} 1 & \text{si } \sigma(i) < \sigma(j) \\ -1 & \text{si } \sigma(i) > \sigma(j). \end{cases}$$

Definimos además la función

$$\mathrm{sig} : \mathrm{Sym}(n) \longrightarrow \{-1,1\}$$

denominada `signo` de la siguiente manera:

$$\mathrm{sig}(\sigma) = \prod_{t\in\mathcal{T}} \zeta_\sigma(t). \tag{3.1}$$

3.2.2 Lema. Para $n \geq 2$ la función

$$\mathrm{sig} : (\mathrm{Sym}(n), \circ) \longrightarrow (\{-1,1\}, \cdot)$$

es un homomorfismo de grupos.

Demostración. Es claro que $\mathrm{sig}(\sigma) \in \{-1,1\}$ para todo $\sigma \in \mathrm{Sym}(n)$. Para $\rho \in \mathrm{Sym}(n)$ y $t = \{i,j\} \in \mathcal{T}$ definamos $\rho(t) = \{\rho(i), \rho(j)\}$ y determinemos los valores de $\zeta_\rho(t)$, $\zeta_\sigma(\rho(t))$ y $\zeta_{\sigma\rho}(t)$.

Casos	$\zeta_\rho(t)$	$\zeta_\sigma(\rho(t))$	$\zeta_{\sigma\rho}(t)$
$\rho(i)<\rho(j),\ \sigma(\rho(i))<\sigma(\rho(j))$	1	1	1
$\rho(i)<\rho(j),\ \sigma(\rho(i))>\sigma(\rho(j))$	1	-1	-1
$\rho(i)>\rho(j),\ \sigma(\rho(i))<\sigma(\rho(j))$	-1	-1	1
$\rho(i)>\rho(j),\ \sigma(\rho(i))>\sigma(\rho(j))$	-1	1	-1

Observe que en todos los casos se cumple que

$$\zeta_{\sigma\rho}(t) = \zeta_\rho(t)\zeta_\sigma(\rho(t)).$$

Con esto tenemos

$$\begin{aligned}\operatorname{sig}(\sigma\rho) &= \prod_{t\in\mathcal{T}} \zeta_{\sigma\rho}(t)\\ &= \prod_{t\in\mathcal{T}} \zeta_{\rho}(t)\zeta_{\sigma}(\rho(t))\\ &= \prod_{t\in\mathcal{T}} \zeta_{\sigma}(\rho(t)) \prod_{t\in\mathcal{T}} \zeta_{\rho}(t)\\ &= \operatorname{sig}(\sigma)\ \operatorname{sig}(\rho),\end{aligned}$$

con lo cual se tiene la afirmación. □

3.2.3 Ejemplos. (1) Si I denota la función identidad sobre Ω, entonces $\operatorname{sig}(I) = 1$.

(2) Si $\sigma \in \operatorname{Sym}(n)$, entonces $\operatorname{sig}(\sigma) = \operatorname{sig}(\sigma^{-1})$.

3.2.4 Lema. Sean $\Omega = \{1, \ldots, n\}$ con $n \geq 2$. Si $\tau \in \operatorname{Sym}(n)$ es una transposición, entonces $\operatorname{sig}(\tau) = -1$.

Demostración. Sea inicialmente $\tau = (1, 2)$. Entonces

$$\zeta_{\tau}(t) := \begin{cases} -1 & \text{si } \ t = \{1,2\} \\ 1 & \text{si } \ t \neq \{1,2\}. \end{cases}$$

Por lo tanto, $\operatorname{sig}(\tau) = -1$. Sea ahora τ' una transposición cualquiera, digamos $\tau' = (ij)$. Definamos

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ i & j & \pi(3) & \cdots & \pi(n) \end{pmatrix} \in \operatorname{Sym}(n). \tag{3.2}$$

Entonces se verifica que $\tau' = \pi\tau\pi^{-1}$. En efecto,

$$\pi\tau\pi^{-1}(i) = \pi\tau(\pi^{-1}(i)) = \pi\tau(1) = \pi(2) = j.$$

$$\pi\tau\pi^{-1}(j) = \pi\tau(\pi^{-1}(j)) = \pi\tau(2) = \pi(1) = i.$$

Para $k \neq i, j$ tenemos

$$\pi\tau\pi^{-1}(k) = \pi\tau(\pi^{-1}(k)) = \pi(\pi^{-1}(k)) = k.$$

Con esto tenemos que

$$\operatorname{sig}(\tau') = \operatorname{sig}(\pi)\ \operatorname{sig}(\tau)\ \operatorname{sig}(\pi^{-1}).$$

Dado que $\operatorname{sig}(\pi) = \operatorname{sig}(\pi^{-1})$, se sigue que

$$\operatorname{sig}(\tau') = \operatorname{sig}(\tau) = -1,$$

con lo cual se tiene la afirmación. □

3.2.5 Teorema. Sean $n \geq 2$, K un cuerpo y

$$f : (\mathrm{Sym}(n), \circ) \longrightarrow (K^{\times}, \cdot)$$

un homomorfismo de grupos. Entonces

(1) Si $\mathrm{char}\,(K) = 2$, entonces $f(\sigma) = 1$ para todo $\sigma \in \mathrm{Sym}(n)$.

(2) Si $\mathrm{char}\,(K) \neq 2$, entonces $f = \mathrm{sig}$.

Demostración. Si τ es una transposición, entonces $\tau^2 = I_\Omega$ y se tiene que

$$f(\tau)^2 = f(\tau)f(\tau) = f(\tau^2) = f(I_\Omega) = 1.$$

Por lo tanto, $f(\tau) \in \{-1, 1\}$.

Sea $\tau' = (ij)$ cualquier transposición y π la permutación definida en (3.2). Entonces $\tau' = \pi(12)\pi^{-1}$ y se tiene que

$$f(\tau') = f(\pi)\ f((12))\ f(\pi^{-1}) = f((12)).$$

Esto demuestra que las transposiciones tienen la misma imagen bajo f. Es decir, todas tienen bajo f imagen 1 o todas tienen bajo f imagen -1.

Sea $\sigma \in \mathrm{Sym}(n)$ cualquiera. Del teorema 3.1.4 se sigue que $\sigma = \tau_1 \cdots \tau_k$, donde cada τ_j es una transposición. Del lema anterior se sigue que

$$\mathrm{sig}(\sigma) = \prod_{j=1}^{k} \mathrm{sig}(\tau_j) = (-1)^k. \tag{3.3}$$

Por otro lado,

$$f(\sigma) = \prod_{j=1}^{k} f(\tau_j) = \begin{cases} 1 & \text{si } f(\tau_j) = 1 \\ (-1)^k & \text{si } f(\tau_j) = -1. \end{cases} \tag{3.4}$$

Diferenciamos ahora los dos casos posibles:

(1) Si $\mathrm{char}\,(K) = 2$, entonces $f(\sigma) = 1$ para todo $\sigma \in \mathrm{Sym}(n)$, ya que $-1 = 1$.

(2) Si $\mathrm{char}\,(K) \neq 2$, entonces de (3.3) y (3.4) se sigue que $f = \mathrm{sig}$. □

3.3 El grupo alternante

3.3.1 Definición. Para $n \geq 2$ definimos $\mathrm{Alt}(n) := \ker(\mathrm{sig})$. Esto es,

$$\mathrm{Alt}(n) = \{\sigma \in \mathrm{Sym}(n) \mid \mathrm{sig}(\sigma) = 1\}.$$

$\mathrm{Alt}(n)$ se denomina el `grupo alternante` de grado n. Del corolario anterior se sigue que los elementos de $\mathrm{Alt}(n)$ pueden expresarse como un producto de un número par de transposiciones. Por esta razón, estas son usualmente denominadas permutaciones `pares`. Las permutaciones pertenecientes a $\mathrm{Sym}(n) \setminus \mathrm{Alt}(n)$ se denominan `impares`.

3.3.2 Ejemplos. (1) $\mathrm{Alt}(2) = \{(1)\}$.

(2) $\mathrm{Alt}(3) = \{(1), (123), (132)\}$.

(3) $\mathrm{Alt}(4) = \{(1), (12)(34), (13)(24), (14)(23), (124), (134), (234), (132), (123), (142), (143), (243)\}$.

3.3.3 Teorema. Sea $n \in \mathbb{N}$ con $n \geq 2$. Entonces

(1) $\mathrm{Alt}(n) \lhd \mathrm{Sym}(n)$.

(2) $|\mathrm{Sym}(n) : \mathrm{Alt}(n)| = 2$.

(3) $|\mathrm{Alt}(n)| = \frac{1}{2}n!$

Demostración. (1) Dado que $\mathrm{Alt}(n) = \ker(\mathrm{sig})$, se tiene la normalidad de $\mathrm{Alt}(n)$.

(2) Del primer teorema de isomorfía se tiene que

$$|\mathrm{Sym}(n) : \mathrm{Alt}(n)| = |\mathrm{Sym}(n)/\mathrm{Alt}(n)| = |\mathrm{Im}(\mathrm{sig})| = 2,$$

con lo cual se tiene la afirmación.

(3) Se sigue de (2) y del teorema de Lagrange. □

3.3.4 Lema. Si $N < G$ con $|G : N| = 2$, entonces $g^2 \in N$ para todo $g \in G$.

Demostración. Si $g \in N$, entonces la afirmación es inmediata. Supongamos que $g \notin N$. Entonces $gN \neq N$. Si $g^2 \notin N$, entonces $g^2N \neq N$, y se debe verificar que $g^2N = gN$. Esto trae como consecuencia que $gN = N$, lo cual no es posible. □

El siguiente teorema es de gran importancia a la hora de establecer un contraejemplo sobre la no existencia en general de subgrupos cuyos ordenes sean números que dividen el orden del grupo. La prueba que presentamos del teorema se debe a T. L. Sheu.

3.3.5 Teorema. El grupo Alt(4) no tiene subgrupos de orden 6.

DEMOSTRACIÓN. Supongamos que G admite un subgrupo de orden 6, digamos N. Entonces $|G : N| = 2$, y del lema 3.3.4 se tendría que $g^2 \in N$ para todo $g \in \mathrm{Alt}(4)$. Si g es un 3-ciclo, entonces

$$g = g^4 = (g^2)^2 \in N.$$

Dado que en Alt(4) existen ocho 3-ciclos, se tendrían 8 elementos en N, lo cual es una contradicción. □

El grupo alternante $\mathrm{Alt}(n)$ para $n \geq 5$ es de especial interés, ya que estos suministran la primera serie de grupos simples. Los grupos simples juegan un papel importante en el estudio de los grupos solubles.

3.3.6 Lema. Si $n \geq 3$, entonces $\mathrm{Alt}(n)$ es generado por los 3-ciclos de $\mathrm{Sym}(n)$.

DEMOSTRACIÓN. Dado que cada elemento de $\mathrm{Alt}(n)$ es expresable como el producto de un número par de transposiciones, es suficiente demostrar que el producto de dos transposiciones es un producto de 3-ciclos.

En el análisis de los diferentes casos, letras diferentes representan números diferentes.

Caso 1. $(1) = (xy)(xy) = (123)(123)(123)$.

Caso 2. $(xy)(yz) = (xyz)$.

Caso 3. $(xy)(zw) = (xy)(yz)(yz)(zw) = (xyz)(yzw)$. □

3.3.7 Lema. Sean $n \geq 5$ y $N \trianglelefteq \mathrm{Alt}(n)$. Si N contiene un 3-ciclo, entonces $N = \mathrm{Alt}(n)$.

DEMOSTRACIÓN. Supongamos que N contiene un 3-ciclo, digamos (abc). Sea (xyz) otro 3-ciclo cualquiera y $\pi \in \mathrm{Sym}(n)$ con

$$\begin{aligned} \pi(a) &= x, \\ \pi(b) &= y, \\ \pi(c) &= z. \end{aligned}$$

Entonces

$$\pi(abc)\pi^{-1} = (xyz). \tag{3.5}$$

`Caso 1.` Si π es una permutación par, entonces $(xyz) \in N$ y del lema 3.3.6 se tiene la afirmación.

`Caso 2.` Si π es una permutación impar, entonces, dado que $n \geq 5$, existen $v, w \in \{1, \ldots, n\} \setminus \{x, y, z\}$ y podemos reemplazar a π en (3.5) por la permutación par $\tau = \pi(vw)$. Note que

$$\tau(abc)\tau^{-1} = (xyz)$$

y, en consecuencia, todo 3-ciclo pertenece a N. Nuevamente del lema 3.3.6 se sigue la afirmación. □

3.3.8 Lema. Sean $n \geq 5$ y $N \lhd \mathrm{Alt}(n)$. Entonces no existe en N un elemento cuya descomposición en cílcos disyuntos tenga un ciclo con longitud mayor o igual a 4.

Demostración. Supongamos que existe $\pi \in N$, cuya descomposición en ciclos disyuntos tiene un ciclo con longitud por lo menos 4. Dado que ciclos disyuntos conmutan, no se pierde generalidad si suponemos que

$$\pi = (a_1 a_2 \ldots a_k)\sigma_2 \cdots \sigma_m,$$

con $k \geq 4$. Si definimos τ de la siguiente manera:

$$\tau := (a_1\ a_2\ a_3)\pi(a_1\ a_2\ a_3)^{-1},$$

entonces

$$\tau = (a_2\ a_3\ a_1\ a_4 \cdots a_k)\sigma_2 \cdots \sigma_m \in N,$$

y se verifica que

$$\tau\pi^{-1} = (a_1\ a_2\ a_4) \in N.$$

Del lema anterior se sigue que $N = \mathrm{Alt}(n)$, lo cual no es posible. □

3.3.9 Observación. Sean $n \geq 5$ y $N \lhd \mathrm{Alt}(n)$. Como consecuencia del lema anterior se tiene que en la descomposición en ciclos disyuntos de los elementos de N aparecen ciclos con longitud 2 o 3. Mas aun, no es posible que aparezca un único 3-ciclo en dicha descomposición, ya que de lo contrario se tendría un 3-ciclo en N, lo cual no es posible.

3.3.10 Lema. Sean $n \geq 5$ y $N \lhd \mathrm{Alt}(n)$. Entonces no existe en N un elemento cuya descomposición en cíclos disyuntos tenga dos 3-ciclos.

Demostración. Sea $\pi \in N$ una permutación en cuya descomposición en ciclos disyuntos aparecen por lo menos dos 3-ciclos, digamos

$$\pi = (a_1\ a_2\ a_3)(a_4\ a_5\ a_6)\sigma_2 \cdots \sigma_m.$$

Entonces N tiene como elemento al conjugado

$$\begin{aligned}\tau &:= (a_4\ a_5\ a_3)\pi(a_4\ a_5\ a_3)^{-1} \\ &= (a_1\ a_2\ a_4)(a_3\ a_6\ a_5)\sigma_2 \cdots \sigma_m \in N,\end{aligned}$$

y por lo tanto,

$$\pi\tau = (a_1\ a_3\ a_4\ a_2\ a_5)\cdots \in N,$$

lo cual contradice el lema 3.3.8. □

3.3.11 Teorema. Para $n \geq 5$, el grupo alternante $\mathrm{Alt}(n)$ es simple.

Demostración. Supongamos que $\mathrm{Alt}(n)$ no es simple y sea $1 \neq N \lhd \mathrm{Alt}(n)$. De los lemas 3.3.7, 3.3.8 y 3.3.10 se sigue que todo elemento de N es un producto de un número par de transposiciones disyuntas.

Si $\pi = (ab)(cd) \in N$, entonces para todo $f \notin \{a, b, c, d\}$ se verifica que

$$\begin{aligned}\tau &:= (afb)\pi(afb)^{-1}\\ &= (af)(cd) \in N.\end{aligned}$$

Por lo tanto,

$$\pi\tau = (afb) \in N,$$

lo cual es una contradicción. En consecuencia, si $(1) \neq \pi \in N$, entonces en su descomposición en ciclos disyuntos aparecen por lo menos 4 transposiciones disyuntas.

Sea $\pi \in N$ de la forma

$$\pi = (a_1b_1)(a_2b_2)(a_3b_3)(a_4b_4).$$

Entonces si definimos τ mediante

$$\tau := (a_3b_2)(a_2b_1)\pi(a_2b_1)(a_3b_2),$$

se tiene que

$$\tau = (a_1a_2)(a_3b_1)(b_2b_3)(a_4b_4) \in N.$$

Por lo tanto,

$$\pi\tau = (a_1b_2a_3)(a_2b_1b_3) \in N,$$

lo cual es una contradicción. □

En particular $\mathrm{Alt}(5)$ es simple y este constituye el ejemplo del grupo simple no abeliano de menor orden que existe. Mas aún, todo grupo simple de orden 60 es isomorfo a $\mathrm{Alt}(5)$.

3.4 Ejercicios

1. Demuestre que $\mathrm{Sym}(3) \cong \mathrm{GL}_2(2)$.
2. Considere la permutación $\sigma = (16524783) \in \mathrm{Sym}(8)$:
   (*a*) Descomponga a σ como producto de transposiciones.
   (*b*) Halle $n \in \mathbb{N}$ tal que $\sigma^n = (1)$.
   (*c*) Calcule σ^{900}.
3. Sea $G = \mathrm{Sym}(3)$, $\alpha = (12)$ y $\beta = (132)$. Halle
   (*a*) $\langle\alpha\rangle$
   (*b*) $\langle\beta\rangle$
   (*c*) $\langle\alpha\rangle\langle\beta\rangle$
   (*d*) $\langle\alpha\rangle \cap \langle\beta\rangle$
4. Sea $G = \mathrm{Sym}(4)$, $\alpha = (1234)$ y $\beta = (14)(32)$. Halle
   (*a*) $\langle\alpha\rangle$
   (*b*) $\langle\beta\rangle$
   (*c*) $\langle\alpha\rangle \cap \langle\beta\rangle$.
5. Sean $n \in \mathbb{N}$ con $n \geq 3$. Demuestre que $\mathrm{Alt}(n)$ es generado por el conjunto
$$\{(12k) \mid k \geq 3\}.$$
6. Sea $\sigma \in \mathrm{Sym}(n)$ y $\sigma = \varepsilon_1 \cdots \varepsilon_k$ su descomposición en ciclos, con
$$\varepsilon_j = (a_j \sigma(a_j) \dots \sigma^{n_j - 1}(a_j)).$$
   Demuestre que $\mathrm{sig}(\sigma) = (-1)^{n-k}$.
7. Sea $n, k \in \mathbb{N}$. Demuestre que
   (*a*) Cada elemento de $\mathrm{Sym}(n)$ puede descomponerse como un número par o impar de transposiciones.
   (*b*) Si σ es un k-ciclo, entonces $\mathrm{sig}(\sigma) = (-1)^{k-1}$.
8. Sea $\alpha = (125)(46)$, $\beta = (15)(234) \in \mathrm{Sym}(6)$. Determine si α y β son conjugados, y en caso que lo sean, halle todas las permutaciones $\sigma \in \mathrm{Sym}(6)$ tales que $\sigma^{-1}\alpha\sigma = \beta$.
9. Demuestre que los únicos subgrupos normales de $\mathrm{Sym}(4)$ son $\mathrm{Sym}(4), \mathrm{Alt}(4)$, el 4-grupo de Klein y 1.

10. Demuestre que los únicos subgrupos normales de $\mathrm{Alt}(4)$ son $\mathrm{Alt}(4)$, el 4-grupo de Klein y 1.

11. Demuestre que $\mathrm{Sym}(n) = \langle (12), (12\cdots n) \rangle$.

12. Demuestre que $\mathrm{Sym}(n) = \langle (12), (13), \cdots, (1n) \rangle$.

13. Demuestre que $\mathrm{Sym}(n) = \langle (12), (23), \cdots, (n-1n) \rangle$.

14. Sea $n \in \mathbb{N}$ con $n \geq 2$, $\pi = (12\cdots n)$ y $\sigma \in \mathrm{Sym}(n)$. Demuestre que $\pi\sigma = \sigma\pi$ si y solo si $\sigma \in \langle \pi \rangle$.

15. Determine $Z(\mathrm{Sym}(n))$ y $Z(\mathrm{Alt}(n))$.

16. Sea $m, n \in \mathbb{N}$ con $n \leq m$. Demuestre que

    (*a*) $\mathrm{Sym}(n)$ es isomorfo a un subgrupo de $\mathrm{Sym}(m)$.

    (*b*) $\mathrm{Alt}(n)$ es isomorfo a un subgrupo de $\mathrm{Alt}(m)$.

17. Demuestre que si $n \geq 3$, entonces $\mathrm{Sym}(n)$ no es abeliano.

18. Demuestre que si $n \geq 4$, entonces $\mathrm{Alt}(n)$ no es abeliano.

19. Demuestre $\mathrm{Sym}(n)$ y $\mathrm{Alt}(n)$ no tienen subgrupos normales de orden dos.

20. Sea $\sigma \in \mathrm{Sym}(n)$ y $\{i_1, \ldots, i_r\} \subseteq \{1, \ldots, n\}$. Demuestre que

$$\sigma(i_1 i_2 \cdots i_r)\sigma^{-1} = (\sigma(i_1)\sigma(i_2)\cdots\sigma(i_r)).$$

21. Demuestre que todo subgrupo de $\mathrm{Sym}(n)$ con índice n es isomorfo a $\mathrm{Sym}(n-1)$.

22. Demuestre que si $n \geq 5$, entonces $\mathrm{Alt}(n)$ es el único subgrupo normal no trivial de $\mathrm{Sym}(n)$.

23. Sea $G = \mathrm{Sym}(4)$ y $N = \{(1), (12)(34), (13)(24), (14)(23)\}$. Demuestre que N es un subgrupo normal de G y determine el grupo G/N.

24. Para $G = \mathrm{Sym}(3)$, $G = \mathrm{Alt}(4)$ y $G = \mathrm{Sym}(4)$ complete la siguiente tabla:

g	$\mathrm{ccl}_G(g)$	$C_G(g)$	$\lvert C_G(g)\rvert$
(1)	G	G	$\lvert G\rvert$
$\vdots$	$\vdots$	$\vdots$	$\vdots$

CAPÍTULO 4

GRUPOS CÍCLICOS

Sea A, B, C,... un conjunto de operaciones que pueden realizarse en un mismo objeto o conjunto de objetos. The Theory of Groups of Finite Order.
(William Burnside - 1897)

A lo largo de este capítulo G denota siempre un grupo. En lo que sigue presentamos algunos resultados importantes sobre grupos cíclicos.

4.1 Elementos de torsión

4.1.1 Definición. (1) Se dice que $g \in G$ es un elemento de `torsión` de G si $\text{ord}(g)$ es finito. Los elementos de G que tienen orden 2 se denominan `involuciones`.

(2) G se llama un grupo `libre de torsión` si todo $1 \neq g \in G$ tiene orden infinito.

4.1.2 Ejemplos. (1) Si G es finito, entonces todos sus elementos son de torsión.

(2) $\mathbb{Z}$ es un grupo libre de torsión. En general, todo grupo libre de torsión debe ser infinito.

(3) Para el 4-grupo de Klein se verifica que todo sus elementos distintos de 1 son involuciones.

(4) Sea p un número primo y

$$\mathbb{Q}_p := \left\{ \frac{a}{p^n} \mid a \in \mathbb{Z},\ n \in \mathbb{N}_0 \right\}.$$

Se verifica que $(\mathbb{Q}_p, +)$ es un grupo abeliano y además libre de torsión. Para demostrar la última afirmación, sea $\frac{a}{p^n} \in \mathbb{Q}_p$ y supongamos que existe $n \in \mathbb{N}$ tal que

$$n\Big(\frac{a}{p^n}\Big) = 0.$$

Entonces $\dfrac{na}{p^n} = 0$ y se sigue que $na = 0$. Por lo tanto, $a = 0$ y se tiene la afirmación.

En el siguiente ejemplo presentamos un grupo infinito en el cual todos sus elementos son de torsión.

4.1.3 Ejemplo. (Grupo de Prüfer[1]) Sea p un número primo y denotemos con $\mathbb{Z}(p^\infty)$ al subconjunto de $\mathbb{C}$ definido de la siguiente manera:

$$\mathbb{Z}(p^\infty) := \{ z \in \mathbb{C} \mid z^{p^n} = 1 \text{ para algún } n \in \mathbb{N}_0 \}.$$

Es decir, $\mathbb{Z}(p^\infty)$ consta de las soluciones complejas de las ecuaciones $x^{p^n} = 1$, donde n recorre el conjunto de los números naturales.

$$\mathbb{Z}(p^\infty) := \left\{ e^{\frac{2\pi i m}{p^n}} \;\middle|\; m, n \in \mathbb{N}_0 \right\}.$$

Se verifica que $(\mathbb{Z}(p^\infty), \cdot)$ es un grupo abeliano infinito en el cual todo elemento tiene orden finito. En efecto, sean $z_1, z_2 \in \mathbb{Z}(p^\infty)$. Entonces existen $n_1, n_2 \in \mathbb{N}$ tales que

$$z_1^{p^{n_1}} = 1 \quad \text{y} \quad z_2^{p^{n_2}} = 1.$$

Si definimos $n := n_1 + n_2$ se tiene que

$$(z_1 z_2)^{p^n} = 1.$$

Esto demuestra que $z_1 z_2 \in \mathbb{Z}(p^\infty)$.

Por otro lado, sea $z \in \mathbb{Z}(p^\infty)$. Entonces existe $n \in \mathbb{N}$ tal que $z^{p^n} = 1$. Sin dificultades se tiene que $(z^{-1})^{p^n} = 1$. Es decir, $z^{-1} \in \mathbb{Z}(p^\infty)$.

[1] Ernst Paul Heinz Prüfer (1896-1934), matemático alemán. Investigó en álgebra y teoría de grupos. En su tesis doctoral abordó el problema de caracterizar los grupos abelianos infinitos con elementos de ordenes finitos.

Lo anterior demuestra que $(\mathbb{Z}(p^\infty),\cdot) \leq (\mathbb{C}^\times,\cdot)$, con lo cual se tiene que $(\mathbb{Z}(p^\infty),\cdot)$ es un grupo abeliano. De la definición de $\mathbb{Z}(p^\infty)$ se sigue que cada uno de sus elementos es de torsión.

Finalmente, si consideramos nuevamente los grupos $U(p^n)$ de las p^n-ésimas raíces complejas de la unidad. Esto es:

$$U(p^n) = \{z \in \mathbb{C} \mid z^{p^n} = 1\},$$

se tiene la siguiente cadena de subgrupos de $\mathbb{C}^\times$:

$$1 = U(p^0) \leq U(p^1) \leq U(p^2) \leq \cdots \leq U(p^n) \leq U(p^{n+1}) \leq \cdots$$

Además

$$\mathbb{Z}(p^\infty) = \bigcup_{n\in\mathbb{N}_0} U(p^n).$$

Una consecuencia del ejemplo anterior es que en el grupo $(\mathbb{C}^\times,\cdot)$ existen elementos de torsión y también elementos con orden infinito.

4.1.4 Teorema. Todo grupo cíclico es abeliano.

Demostración. Sea $G = \langle g\rangle$ y sean $x, y \in G$ cualesquiera. Entonces existen $m, n \in \mathbb{Z}$ tales que $x = g^n$ y $y = g^m$. Por lo tanto,

$$xy = g^n g^m = g^{n+m} = g^{m+n} = g^m g^n = yx,$$

con lo cual se tiene la afirmación. □

Demostramos en el siguiente lema algunas propiedades de los elementos de torsión.

4.1.5 Teorema. Sean $g, h \in G$ y $n, m, k \in \mathbb{N}$. Entonces

(1) Todas las potencias de g son distintas, si y solo si $\operatorname{ord}(g) = \infty$.

(2) $\operatorname{ord}(g) = 1$ si y solo si $g = 1$.

(3) $\operatorname{ord}(g^{-1}) = \operatorname{ord}(g)$.

(4) Si $\operatorname{ord}(gh)$ es finito, entonces $\operatorname{ord}(gh) = \operatorname{ord}(hg)$.

Demostración. (1) Supongamos que todas las potencias de g son distintas. Es decir, $g^i \neq g^j$ para todo $i \neq j$. Entonces es inmediato que $\operatorname{ord}(g) = \infty$.

Recíprocamente, supongamos que no todas las potencias de g son distintas. Es decir, supongamos que existen $l, m \in \mathbb{N}$ tales que $g^l = g^m$. Sin perder generalidad supongamos que $l < m$. Entonces $g^{m-l} = 1$, con $m - l > 0$ y, en consecuencia, el conjunto

$$M = \{k \mid k \in \mathbb{N},\ g^k = 1\} \subseteq \mathbb{N}$$

es no vacío y tiene, por el principio de buen orden, un elemento mínimo, digamos t. Es decir, $g^t = 1$ y, por lo tanto, $\text{ord}(g) < \infty$.

(2) Si $\text{ord}(g) = 1$, entonces $g^1 = g = 1$. Recíprocamente, si $g = 1$, entonces $g^1 = 1^1 = 1$ y se tiene que $\text{ord}(g) = 1$.

(3) Es suficiente observar que

$$(g^{-1})^m = 1 \Leftrightarrow (g^m)^{-1} = 1 \Leftrightarrow g^m = 1.$$

(4) Supongamos que $\text{ord}(gh) = m$. Entonces

$$\begin{aligned}(gh)^m = 1 &\Leftrightarrow g(hg)^{m-1}h = 1\\ &\Leftrightarrow (hg)^{m-1} = g^{-1}h^{-1}\\ &\Leftrightarrow (hg)^{m-1} = (hg)^{-1}\\ &\Leftrightarrow (hg)^m = 1. \quad \square\end{aligned}$$

4.1.6 Teorema. Sean $k \in \mathbb{N}$ y $g \in G$. Entonces

(1) $g^m = 1$ si y solo si $\text{ord}(g) \mid m$.

(2) $\langle g \rangle = \{1, g, \ldots, g^{n-1}\}$. En particular $|\langle g \rangle| = \text{ord}(g)$.

(3) $\text{ord}(g) \mid |G|$ y $g^{|G|} = 1$.

(4) $\text{ord}(g^k) = \frac{\text{ord}(g)}{\text{mcd}(n,k)}$.

Demostración. Supongamos que $\text{ord}(g) = n$.

(1) Si $g^m = 1$, entonces aplicando el algoritmo de la división con resto tenemos que $m = nq + r$, con $0 \leq r < n$. Entonces

$$1 = g^m = (g^n)^q g^r = g^r$$

Por la minimalidad de n se tiene que $r = 0$, y así $m = nq$.

Recíprocamente, si $n \mid m$, entonces $m = nq$, y se sigue que

$$g^m = g^{nq} = (g^n)^q = 1.$$

(2) Recordemos que $\langle g\rangle = \{g^m \mid m \in \mathbb{Z}\}$. Sea ahora $m \in \mathbb{Z}$ cualquiera. Usando el algoritmo de la división con resto se tiene que $m = qn + r$, con $0 \le r < n$. Entonces

$$g^m = g^{qn+r} = (g^n)^q g^r = g^r.$$

Por lo tanto, $\langle g\rangle = \{1, g, \ldots, g^{n-1}\}$. Resta demostrar que todos los elementos de $\langle g\rangle$ son distintos dos a dos.

Supongamos que $g^i = g^j$, con $0 \le i \le j < n$. Entonces $g^{j-i} = 1$ y se tiene $n \mid (j-i)$, lo cual se verifica si y solo si $j - i = 0$. Es decir, si y solo si $i = j$.

(3) Dado que $|\langle g\rangle| = \operatorname{ord}(g)$, del teorema de Lagrange se sigue la afirmación. Por otro lado, $|G| = \operatorname{ord}(g)k$ para algún $k \in \mathbb{N}$. Por lo tanto,

$$g^{|G|} = (g^{\operatorname{ord}(g)})^k = 1.$$

(4) Dado que n divide a $\frac{nk}{\operatorname{mcd}(n,k)}$, se sigue inmediatamente que

$$1 = g^{\frac{nk}{\operatorname{mcd}(n,k)}} = (g^k)^{\frac{n}{\operatorname{mcd}(n,k)}}.$$

Entonces de (2) se sigue que

$$\operatorname{ord}(g^k) \mid \tfrac{n}{\operatorname{mcd}(n,k)}. \tag{4.1}$$

Si $t := \operatorname{ord}(g^k)$, entonces $(g^k)^t = g^{kt} = 1$. Es decir, $n \mid kt$, y naturalmente

$$\tfrac{n}{\operatorname{mcd}(n,k)} \mid \tfrac{kt}{\operatorname{mcd}(n,k)}.$$

Entonces $\frac{n}{\operatorname{mcd}(n,k)} \mid t$. Es decir,

$$\tfrac{n}{\operatorname{mcd}(n,k)} \mid \operatorname{ord}(g^k). \tag{4.2}$$

De (4.1) y (4.2) se sigue la igualdad. □

4.1.7 Teorema. Sean $g, h \in G$. Si g y h son elementos de torsión y $gh = hg$, entonces

$$\operatorname{ord}(gh) \mid \operatorname{mcm}(\operatorname{ord}(g), \operatorname{ord}(h)).$$

Si además $\operatorname{mcd}(\operatorname{ord}(g), \operatorname{ord}(h)) = 1$, entonces

$$\operatorname{ord}(gh) = \operatorname{ord}(g)\operatorname{ord}(h).$$

Demostración. Sea $M := \text{mcm}(\text{ord}(g), \text{ord}(h))$. Si $gh = hg$, entonces

$$(gh)^M = g^M h^M = 1.$$

Por lo tanto, $\text{ord}(gh) \mid M$.

Sean $m := \text{ord}(g)$, $n := \text{ord}(h)$ y $k := \text{ord}(gh)$. Dado que g y h conmutan, se tiene nuevamente que

$$(gh)^{mn} = g^{mn}h^{mn} = (g^m)^n(h^n)^m = 1,$$

y, en consecuencia, $k \mid mn$.

Por otro lado,

$$\begin{aligned}(gh)^k = g^k h^k = 1 &\Leftrightarrow g^k = h^{-k} \\ &\Rightarrow \text{ord}(g^k) = \text{ord}(h^{-k}) = \text{ord}(h^k) \\ &\Leftrightarrow \tfrac{m}{\text{mcd}(m,k)} = \tfrac{n}{\text{mcd}(n,k)} \\ &\Rightarrow m \mid k \ \text{ y } \ n \mid k \\ &\Rightarrow mn \mid k.\end{aligned}$$

En conclusión, $k = mn$. Es decir, $\text{ord}(gh) = \text{ord}(g)\text{ord}(h)$. □

4.1.8 Corolario. Sean $g, h \in G$. Entonces $\text{ord}(g) = \text{ord}(hgh^{-1})$.

Demostración. Supongamos que $\text{ord}(g) = n$. Note que

$$(hgh^{-1})^n = hg^n h^{-1} = h1h^{-1} = 1.$$

En consecuencia,

$$\text{ord}(hgh^{-1}) \mid n.$$

Supongamos ahora que $\text{ord}(hgh^{-1}) = k < n$. Entonces

$$1 = (hgh^{-1})^k = hg^k h^{-1}.$$

Por lo tanto, $g^k = 1$, lo cual es una contradicción. □

4.1.9 Corolario. Si $|G|$ es un número primo, entonces G es cíclico.

Demostración. Sea $1 \neq g \in G$. Entonces $1 \neq \text{ord}(g) \mid |G|$. Dado que $|G|$ es un número primo, se tiene que $\text{ord}(g) = |G|$, y así $G = \langle g \rangle$. □

4.2 Subgrupos de grupos cíclicos

4.2.1 Teorema. Subgrupos de grupos cíclicos son cíclicos.

DEMOSTRACIÓN. Sea G un grupo cíclico, digamos $G = \langle g \rangle$ y $U \leq G$.

Si $U = 1$, entonces la afirmación es inmediata.

Sea entonces $U \neq 1$. Dado que $U \subseteq G$, se tiene que todos sus elementos son potencias de g. Sea $1 \neq u \in U$. Entonces existe $0 \neq m \in \mathbb{Z}$ tal que $u = g^m$. Note que

$$g^m \in U \Leftrightarrow (g^m)^{-1} = (g^{-1})^m = g^{-m} \in U.$$

Entonces se tiene que el conjunto

$$M := \{n \in \mathbb{N} \mid g^n \in U\} \neq \varnothing$$

y por el principio de buen orden M tiene un elemento mínimo, digamos k. Demostramos que

$$U = \langle g^k \rangle.$$

Sea $g^s \in U$. Entonces existen $q, r \in \mathbb{Z}$ tal que $s = qk + r$, con $0 \leq r < k$. Por tanto,

$$g^r = g^{s-qk} = g^s g^{-qk} = g^s (g^k)^{-q} \in U.$$

Por la minimalidad de k se tiene entonces que $r = 0$. Entonces $s = qk$ y se sigue que $g^s = (g^k)^q \in \langle g^k \rangle$. Esto demuestra que $U \leq \langle g^k \rangle$.

Recíprocamente, dado que $g^k \in U$, se tiene que $g^{kn} = (g^k)^n \in U$ para todo $n \in \mathbb{Z}$. Entonces $\langle g^k \rangle \leq U$ y se demuestra la primera afirmación. □

4.2.2 Observación. En general, si G es finito y $d \mid |G|$, entonces no siempre se verifica que existe un subgrupo U de G con la propiedad $|U| = d$. Por ejemplo, $\mathrm{Alt}(4)$ no tiene subgrupos de orden 6 a pesar de que 6 divide a $|\mathrm{Alt}(4)| = 12$. No obstante, para grupos cíclicos y para grupos abelianos la afirmación es cierta.

4.2.3 Teorema. Sea $G = \langle g \rangle$ un grupo cíclico.

(1) Si G es infinito, entonces para cada $k \in \mathbb{N}_0$ se verifica que $U_k := \langle g^k \rangle$ es un subgrupo de G, y además estos son todos los subgrupos de G. Adicionalmente, para cada $k \in \mathbb{N}$ se cumple que $|G : U_k| = k$. En particular se cumple que si $k \neq l$, entonces $U_k \neq U_l$.

(2) Si G es finito, digamos $|G| = n$, entonces para todo divisor positivo d de n existe un único subgrupo con d elementos. Estos son concretamente $U_d := \langle g^{\frac{n}{d}} \rangle$.

DEMOSTRACIÓN. (1) La primera afirmación es inmediata, se sigue del teorema anterior.

Para demostrar que $|G : U_k| = k$, probamos que los elementos $e = g^0, g, \ldots, g^{k-1}$ forman un transversal izquierdo para U_k en G.

Para cada $m \in \mathbb{Z}$ existen $s, t \in \mathbb{Z}$ tales que $m = tk + s$ con $0 \leq s < k$. Entonces $g^m = g^s(g^k)^t \in g^s U_k$, y con esto se tiene

$$G = \bigcup_{s=0}^{k-1} g^s U_k.$$

Sea $h \in (g^s U_k \cap g^{s'} U_k)$ con $0 \leq s \leq s' \leq k-1$. Entonces existen $t, t' \in \mathbb{Z}$ tales que

$$h = g^{kt+s} = g^{kt'+s'}.$$

Por lo tanto, $g^{s'-s} = g^{k(t-t')}$. Dado que G es infinito, debe cumplirse que $s' - s = k(t - t')$, y dado que $0 \leq s \leq s' \leq k-1$, se sigue forzosamente que $s = s'$.

(2) Definamos $c := \frac{n}{d}$ y $U_d := \langle g^c \rangle$. Del teorema 4.1.6 se sigue que

$$\operatorname{ord}(g^c) = \frac{n}{\operatorname{mcd}(n, c)} = \frac{n}{\operatorname{mcd}\left(n, \frac{n}{d}\right)} = \frac{n}{\frac{n}{d}} = d.$$

Entonces $|U_d| = |\langle g^c \rangle| = \operatorname{ord}(g^c) = d$.

Sea $V \leq G$ cualquiera, digamos $V = \langle g^k \rangle$, con $\operatorname{ord}(g^k) = d$. Demostramos que $V \leq U_d$.

Del teorema de Lagrange se sigue que $d \mid n$. Por otro lado, de $g^{kd} = 1$ se sigue que $n \mid kd$. Es decir, existe $m \in \mathbb{Z}$ tal que $kd = mn$. Entonces $k = \frac{mn}{d}$ y se sigue que

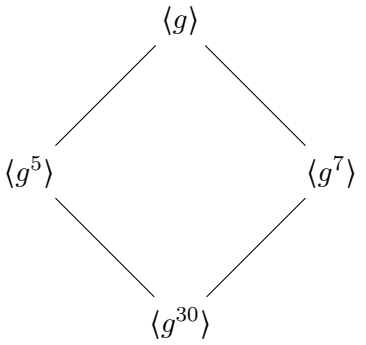
$$g^k = (g^{\frac{n}{d}})^m \in U_d.$$

Por tanto, $V \leq U_d$. Dado que $|V| = d = |U_d|$, se tiene que $V = U_d$. □

4.2.4 Ejemplo. Sea $G = \langle g \rangle$ un grupo cíclico con $|G| = 35$. Entonces los divisores positivos de $|G|$ son 1, 7, 5 y 35. Del teorema anterior se sigue que G admite subgrupos con estos órdenes. Estos subgrupos están dados, respectivamente, por

$$1 = \langle g^{35} \rangle, \langle g^7 \rangle, \langle g^5 \rangle \quad \text{y} \quad \langle g^1 \rangle = G.$$

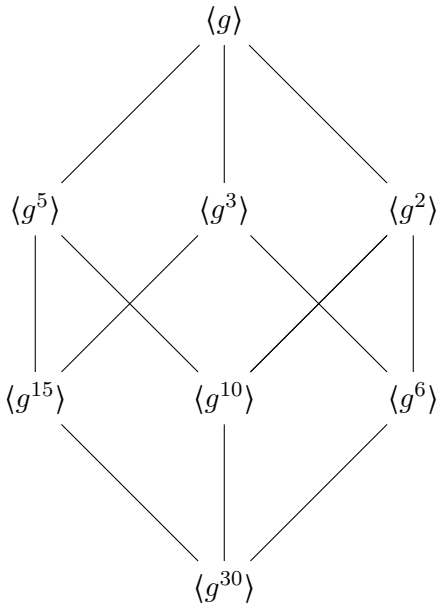
El siguiente diagrama muestra el retículo de todos los subgrupos de G.



4.2.5 Ejemplo. Sea $G = \langle g \rangle$ un grupo cíclico con $|G| = 30$. Entonces los divisores positivos de $|G|$ son 1, 2, 3, 5, 6, 10, 15 y 30. Con base en el teorema anterior se tiene que G admite subgrupos con estos órdenes. Estos subgrupos están dados, respectivamente, por

$$1 = \langle g^{30} \rangle, \langle g^{15} \rangle, \langle g^{10} \rangle, \langle g^6 \rangle, \langle g^5 \rangle, \langle g^3 \rangle, \langle g^2 \rangle \quad \text{y} \quad \langle g^1 \rangle = G.$$

En el siguiente diagrama representamos el retículo de todos los subgrupos de G.



4.3 Clasificación de los grupos cíclicos

Demostramos ahora que salvo isomorfía existen dos tipos de grupos cíclicos, y además la clasificación depende exclusivamente del orden del grupo.

4.3.1 Teorema. Sea G un grupo cíclico.

(1) Si $|G| = \infty$, entonces $G \cong \mathbb{Z}$.

(2) Si $|G| = n$, entonces $G \cong \mathbb{Z}_n$.

DEMOSTRACIÓN. Sea $G = \langle g \rangle$ y $\alpha : \mathbb{Z} \longrightarrow G$ definida por $\alpha(i) := g^i$. Entonces

α es un homomorfismo: $\alpha(i+j) = g^{i+j} = g^i g^j = \alpha(i)\alpha(j)$.

α es un epimorfismo: Sea $x \in G$. Dado que G es cíclico, se tiene que $x = g^j$ para algún $j \in \mathbb{Z}$. Entonces $x = \alpha(j)$.

(1) Sea $|G| = \infty$. Entonces

$$i \in \ker(\alpha) \Leftrightarrow g^i = 1 \Leftrightarrow i = 0.$$

Es decir, α es un isomorfismo.

(2) Sea $|G| = n$. Entonces

$$i \in \ker(\alpha) \Leftrightarrow g^i = 1 \Leftrightarrow n \mid i \Leftrightarrow i \in n\mathbb{Z}.$$

Del primer teorema de isomorfía se sigue que

$$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\ker(\alpha) \cong \mathrm{Im}(\alpha) = G. \quad \square$$

4.3.2 Teorema. Sea $G = \langle g \rangle$. Entonces

(1) Si G es infinito, entonces g y g^{-1} son los únicos generadores de G.

(2) Si G es finito, digamos $|G| = n$, entonces los generadores de G son los elementos de la forma g^k, con $\mathrm{mcd}(k, n) = 1$.

DEMOSTRACIÓN. (1) Para todo $k \in \mathbb{Z}$ se verifica que $\langle g^k \rangle = \langle g^{-k} \rangle$. En particular se tiene que $\langle g \rangle = \langle g^{-1} \rangle = G$. Si $k \neq \pm 1$, entonces del teorema 4.2.3 se sigue que $\langle g^k \rangle = U_{|k|} \neq U_1 = G$.

(2) Sea G finito con $|G| = n$. Entonces

$$\begin{aligned} G = \langle g^k \rangle &\Leftrightarrow \operatorname{ord}(g^k) = n \\ &\Leftrightarrow \frac{n}{\operatorname{mcd}(n,k)} = n \\ &\Leftrightarrow \operatorname{mcd}(n,k) = 1. \qquad \square \end{aligned}$$

4.3.3 Ejemplo. (1) Los únicos generadores de $\mathbb{Z}$ son 1 y -1.

(2) Si $G = \mathbb{Z}_8$, entonces $1, 3, 5$ y 7 generan a G.

4.3.4 Observación. Sea $G = \langle g \rangle$ un grupo cíclico con $|G| = n$. Entonces los elementos que generan a G son de la forma g^k con $1 \leq k \leq n$ y $\operatorname{mcd}(k,n) = 1$. El número de primos relativos con n que están entre 1 y n está dado por la denominada `función de Euler` de la teoría de números, la cual se denota con φ.

Para un número primo p y $m \in \mathbb{N}$ se verifica que

$$\varphi(p^m) = p^m - p^{m-1} = p^{m-1}(p-1).$$

Por otro lado, si $\operatorname{mcd}(m,n) = 1$, entonces $\varphi(mn) = \varphi(m)\varphi(n)$. Por lo tanto, de $n = \prod_{i=1}^{s} p_i^{m_i}$, con $p_1, \ldots, p_s$ primos distintos, se sigue que

$$\varphi(n) = \prod_{i=1}^{s} p_i^{m_i - 1}(p_i - 1).$$

4.3.5 Teorema. Sea $G = \langle g \rangle$ con $|G| = rs$ y $\operatorname{mcd}(r,s) = 1$. Entonces existen $U, V \leq G$ tales que $|U| = r$, $|V| = s$ y $U \cap V = 1$.

Demostración. Definamos $U := \langle g^s \rangle$ y $V := \langle g^r \rangle$. Es claro que $U, V \leq G$. Por otro lado,

$$\begin{aligned} |U| &= \frac{rs}{\operatorname{mcd}(rs,s)} \\ &= \frac{rs}{s \operatorname{mcd}(r,1)} \\ &= r. \end{aligned}$$

De manera similar se demuestra que $|V| = s$.

Sea $x \in (U \cap V)$. Entonces $\operatorname{ord}(x) \mid r$ y $\operatorname{ord}(x) \mid s$. Dado que $\operatorname{mcd}(r,s) = 1$, se tiene que $\operatorname{ord}(x) = 1$ y, por lo tanto, $x = 1$. $\square$

4.4 El grupo de automorfismos de un grupo cíclico

Consideremos ahora el problema de caracterizar el grupo de automorfismos de un grupo cíclico. Dado que G es abeliano, el grupo de automorfismos interiores de G es trivial. Entonces la búsqueda se orienta en la dirección opuesta.

4.4.1 Lema. Sea $n \in \mathbb{N}$.

(1) Si G es abeliano, entonces la función $\alpha : G \longrightarrow G$ definida por $\alpha(g) = g^n$ es un endomorfismo de G.

(2) Si G es abeliano y finito con $\text{mcd}(n, |G|) = 1$, entonces la función α definida arriba es un automorfismo de G.

Demostración. (1) Sean $g, h \in G$. Entonces $\alpha(gh) = (gh)^n = g^n h^n = \alpha(g)\alpha(h)$ y se tiene que α es un endomorfismo.

(2) Es suficiente demostrar que α es inyectiva. Si $g \in \ker(\alpha)$, entonces $g^n = 1$ y se tiene que $\text{ord}(g) \mid n$. Dado que $\text{ord}(g) \mid |G|$ y $\text{mcd}(n, |G|) = 1$, se sigue que $\text{ord}(g) = 1$ y, por lo tanto, $g = 1$. □

4.4.2 Teorema. Sea $G = \langle g \rangle$.

(1) Si $|G| = \infty$, entonces $\text{Aut}(G) \cong \mathbb{Z}_2$.

(2) Si $|G| = n$ y para cada k con $1 \leq k \leq n$ definimos $\alpha_k : G \longrightarrow G$ mediante

$$\alpha_k(g^i) = g^{ik}, \quad \text{para todo} \quad i \in \mathbb{Z},$$

entonces

$$\text{Aut}(G) = \{\alpha_k \mid \text{mcd}(k, n) = 1\}.$$

En particular $\text{Aut}(G)$ es abeliano y tiene orden $\varphi(n)$.

Demostración. (1) Sea $\alpha \in \text{Aut}(G)$ cualquiera. Demostramos que $G = \langle \alpha(g) \rangle$. Es claro que $\langle \alpha(g) \rangle \subseteq G$. Por otro lado, sea $x \in G$ cualquiera. Dado que α es sobreyectiva, existe $y \in G$ tal que

$$x = \alpha(y) = \alpha(g^k) = \alpha(g)^k$$

para algún $k \in \mathbb{Z}$ y se tiene que $G \subseteq \langle \alpha(g) \rangle$. Entonces $G = \langle \alpha(g) \rangle$. Usando el teorema 4.3.2 (1) se tiene que $\alpha(g) = g$ o $\alpha(g) = g^{-1}$ y ambos son automorfismos de G.

(2) Del lema 4.4.1 (2) se sigue que $\alpha_k \in \mathrm{Aut}(G)$ para todo $1 \leq k \leq n$, con $\mathrm{mcd}(k,n) = 1$. Por lo tanto, $\alpha_k \neq \alpha_l$ para todo $1 \leq k < l \leq n$, con $\mathrm{mcd}(n,k) = \mathrm{mcd}(n,l) = 1$.

Sea ahora $\alpha \in \mathrm{Aut}(G)$ cualquiera. Entonces $\alpha(g) = g^m$ para algún $m \in \mathbb{Z}$. Usando la división con resto se tiene que existen $q, k \in \mathbb{Z}$ tales que $m = nq + k$, con $1 \leq k < n$. Entonces

$$\alpha(g) = g^{nq+k} = (g^n)^q g^k = g^k.$$

Es decir, $\alpha = \alpha_k$ para algún $1 \leq k < n$. Como en (1) se tiene que $G = \langle g^k \rangle$ y del teorema 4.3.2 (2) se sigue que $\mathrm{mcd}(n,k) = 1$. □

4.4.3 Ejemplo. Sea $n \in \mathbb{N}$. Dado que $\mathbb{Z}_n = \langle 1 \rangle$, como consecuencia del teorema anterior y teniendo en cuenta la notación aditiva para el grupo, se verifica que

$$\mathrm{Aut}(\mathbb{Z}_n) = \big\{\alpha_k \mid \mathrm{mcd}(k,n) = 1\big\},$$

donde para todo $0 \leq m < n$ se tiene que

$$\alpha_k(m) = \alpha_k(m1) = mk1 = km.$$

Como casos particulares tenemos que

(1) $\mathrm{Aut}(\mathbb{Z}_2) = 1$.

(2) $\mathrm{Aut}(\mathbb{Z}_3) = \{(1), \alpha_2\}$, donde $\alpha_2(x) = 2x$,

(3) $\mathrm{Aut}(\mathbb{Z}_4) = \{(1), \alpha_3\}$, donde $\alpha_3(x) = 3x$,

(4) $\mathrm{Aut}(\mathbb{Z}_5) = \{(1), \alpha_2, \alpha_3, \alpha_4\}$, donde $\alpha_4(x) = 4x$,

4.4.4 Teorema. Sea $n \in \mathbb{N}$. Entonces $\mathrm{Aut}(\mathbb{Z}_n)$ es isomorfo al grupo multiplicativo de las unidades de $\mathbb{Z}_n$. Es decir, al conjunto de los elementos invertibles de $\mathbb{Z}_n$.

Demostración. Se deja como ejercicio. □

4.4.5 Teorema. Sea $G = \langle g \rangle$, $|G| = p^n$, con p un número primo. Entonces

(1) $G = \langle g^k \rangle$ si y solo si $\mathrm{mcd}(k,p) = 1$.

(2) $\mathrm{Aut}(G) = \big\{\alpha_k \mid 1 \leq k \leq p^n \text{ y } \mathrm{mcd}(k,p) = 1\big\}$, con α_k dado por el teorema anterior.

(3) $|\mathrm{Aut}(G)| = p^{n-1}(p-1)$.

(4) $\mathrm{Aut}(G)$ es un grupo abeliano y $\mathrm{Aut}(G) \cong U(\mathbb{Z}_{p^n})$, donde $U(\mathbb{Z}_{p^n})$ denota el grupo multiplicativo de las unidades de $\mathbb{Z}_{p^n}$.

Demostración. (1) Usando el teorema 4.1.6 tenemos

$$G = \langle g^k \rangle \Leftrightarrow \text{mcd}(k, p^n) = 1 \Leftrightarrow \text{mcd}(k, p) = 1.$$

(2) Se sigue del teorema 4.4.2 (2).

(3) $|\text{Aut}(G)| = \varphi(p^n) = p^{n-1}(p-1)$.

(4) Sea $g \in G$. Entones

$$\alpha_k \alpha_l(g) = g^{kl} = g^{lk} = \alpha_l \alpha_k(g).$$

Esto demuestra que $\text{Aut}(G)$ es abeliano.

Recordemos que $\mathbb{Z}_{p^n}^{\times}$ está dado por

$$\mathbb{Z}_{p^n}^{\times} = \left\{ k + p^n\mathbb{Z} \mid \text{mcd}(k, p) = 1 \right\}.$$

Sea

$$\tau : (\text{Aut}(G), \circ) \longrightarrow (\mathbb{Z}_{p^n}^{\times}, \cdot)$$

definida por

$$\tau(\alpha_k) := k + p^n\mathbb{Z}.$$

Demostramos que τ es un homomorfismo. Sean $\alpha_k, \alpha_l \in \text{Aut}(G)$. Entonces

$$\begin{aligned} \tau(\alpha_k \alpha_l) &= \tau(\alpha_{kl}) \\ &= kl + p^n\mathbb{Z} \\ &= (k + p^n\mathbb{Z})(l + p^n\mathbb{Z}) \\ &= \tau(\alpha_k)\tau(\alpha_l). \end{aligned}$$

Demostramos que τ es uno a uno. Supongamos que $\tau(\alpha_k) = \tau(\alpha_l)$. Note que

$$\begin{aligned} \tau(\alpha_k) = \tau(\alpha_l) &\Leftrightarrow k + p^n\mathbb{Z} = l + p^n\mathbb{Z} \\ &\Leftrightarrow (k - l) \in p^n\mathbb{Z} \\ &\Leftrightarrow k = l + p^n m \text{ para algún } m \in \mathbb{Z}. \end{aligned}$$

En consecuencia para todo $g \in G$ se verifica que

$$\alpha_k(g) = g^k = g^l (g^{p^n})^m = g^l = \alpha_l(g).$$

Esto demuestra que $\alpha_k = \alpha_l$ y se tiene la afirmación.

Demostramos que τ es invertible. Note que $\text{mcd}(k, p^n) = 1$ si y solo si existen $\mu, \lambda \in \mathbb{Z}$ tales que $\mu k + \lambda p^n = 1$. Entonces $\mu k \equiv 1 \mod p^n$, con lo cual se garantiza la existencia de la inversa de τ. □

4.5 Ejercicios

1. Demuestre el teorema 4.4.4.
2. ¿Cuántos generadores admite un grupo cíclico de orden 50?
3. Sea G un grupo finito. Demuestre que si G es abeliano y $|G| = pq$, donde p y q son primos distintos, entonces G es cíclico.
4. Sea G un grupo abeliano finito. Demuestre que G tiene un elemento cuyo orden es
$$\exp(G) = \operatorname{mcm}\{\operatorname{ord}(x) \mid x \in G\}.$$
5. Sea G un grupo y $n \in \mathbb{N}$. Demuestre que si G admite un único elemento g de orden n, entonces $g \in Z(G)$ y $n = 2$.
6. Determine el número de generadores de un grupo cíclcio de orden 70.
7. Sea G y H grupos, $\varphi \in \operatorname{Hom}(G, H)$ y $g \in G$ un elemento de torsión. Demuestre que
$$\operatorname{ord}(\varphi(g)) \mid \operatorname{ord}(g).$$
¿Cuándo se verifica la igualdad?
8. Demuestre que en todo grupo finito de orden par el número de involuciones es impar.
9. Demuestre que un grupo abeliano finito es simple si y solo si su orden es 1 o un número primo.
10. Sea G un grupo de orden impar. Demuestre que para todo $g \in G$ existe $h \in G$ tal que $h^2 = g$.
11. Determine el número de monomorfismos que existen de $\mathbb{Z}_3$ en $\operatorname{Sym}(3)$.
12. Demuestre que el conjunto de elementos de torsión de un grupo abeliano G es un subgrupo de G.
13. Dibuje el retículo de subgrupos de un grupo cíclico de orden p^2q, donde p y q son números primos distintos.
14. Dibuje el retículo de subgrupos de un grupo cíclico de orden 60.
15. Sean $m, n \in \mathbb{Z}$, $d := \operatorname{mcd}(a, b)$ y $k := \operatorname{mcm}(m, n)$. Demuestre que
   (*a*) $(\langle n \rangle, +) = (n\mathbb{Z}, +)$ es un grupo cíclcio.
   (*b*) $n\mathbb{Z} + m\mathbb{Z} = \langle d \rangle = d\mathbb{Z}$.

(c) $n\mathbb{Z} \cap m\mathbb{Z} = \langle k \rangle = k\mathbb{Z}$.

16. Sean $a, b, m, n \in \mathbb{Z}$ con $\mathrm{mcd}(a, m) = \mathrm{mcd}(b, n) = 1$, $d := \mathrm{mcd}(a, b)$ y $k := \mathrm{mcm}(m, n)$. Demuestre que

    (a) $(\langle \frac{1}{a}, \frac{1}{b} \rangle, +) = (\langle \frac{d}{ab} \rangle, +) \leq (\mathbb{Q}, +)$.

    (b) $(\langle \frac{a}{m}, \frac{b}{n} \rangle, +) = (\langle \frac{d}{k} \rangle, +) \leq (\mathbb{Q}, +)$.

17. Sea X un subconjunto finito de $\mathbb{Q}$.

    (a) Demuestre que $(\langle X \rangle, +)$ es un grupo cíclico.

    (b) Describa un algoritmo que encuentre $x \in \mathbb{Q}$ tal que $\langle X \rangle = \langle x \rangle$.

    (c) ¿Es $(\mathbb{Q}, +)$ finitamente generado?

18. `Demuestre o refute:` Sea G un grupo y $M, N \trianglelefteq G$.

    (a) Si G es cíclico, entonces G/N también lo es.

    (b) Si G/N y G/M son cíclicos, entonces $G/(M \cap N)$ también lo es.

19. Considere los grupos $\mathbb{Q}$ y $\mathbb{Z}$ aditivamente. Demuestre que $\mathbb{Q}/\mathbb{Z}$ es un grupo infinito, en el cual todo elemento tiene orden finito.

20. Sea G un grupo cíclico y $U \leq G$. Demuestre que U es un subgrupo maximal de G si y solo si $|G : U|$ es un número primo.

21. Sea G un grupo finito. Demuestre que si G tiene un único subgrupo maximal, entonces G es cíclico y $|G|$ es la potencia de algún número primo. Se verifica el recíproco de esta afirmación.

22. Demuestre que un grupo finito abeliano G es cíclico si y solo si $\exp(G) = |G|$.

23. Sea G un grupo tal que el grupo cociente $G/Z(G)$ es cíclico. Demuestre que G es abeliano.

CAPÍTULO 5

PRODUCTOS DIRECTOS Y SEMIDIRECTOS

Dada una o más sustituciones que involucran algunos o todos los elementos $x, y, z, \ldots$, llamamos a los productos de estas sustituciones, entre sí mismas o por cualquier otra, en cualquier orden, sustituciones derivadas. Las sustituciones dadas, junto con las derivadas, forman lo que llamamos un sistema de sustituciones conjugadas.
(Augustin - Louis Cauchy)

En este capítulo se presentan la construcción del producto cartesiano finito o infinito de una familia de grupos, no necesariamente finitos y su suma directa externa. Seguidamente se caracteriza la suma directa interna de una familia de subgrupos de un grupo dado. Posteriormente se demuestra que las nociones de externo e interno son equivalentes. Estas técnicas presentadas constituyen además una forma de construir nuevos grupos a partir de otros dados o para indagar sobre la estructura interna de ciertos grupos.

5.1 Producto directo externo - caso finito

5.1.1 Definición. Sea $J = \{1, \ldots, n\}$ y para cada $j \in J$, sea G_j un grupo, notado multiplicativamente. Consideremos el producto cartesiano (conjuntista) de tales grupos. Esto es,

$$\prod_{j \in J} G_j = G_1 \times \cdots \times G_n = \{(g_1, \ldots, g_n)\} \mid g_j \in G_j\}.$$

Definamos sobre $\prod_{j\in J} G_j$ la siguiente multiplicación:

$$(g_1,\dots,g_n)\cdot(g_1',\dots,g_n') \coloneqq (g_1g_1',\dots,g_ng_n'). \tag{5.1}$$

Entonces $(\prod_{j\in J} G_j,\cdot)$ es un grupo, el cual se denomina `producto cartesiano` de los grupos $\{G_j\}_{j\in J}$.

5.1.2 Observación. Si $J=\{1,\dots,n\}$ y los grupos $G_1,\dots,G_n$ son notados aditivamente, entonces la operación (5.1) se transforma en

$$(g_1,\dots,g_n)+(g_1',\dots,g_n') \coloneqq (g_1+g_1',\dots,g_n+g_n'). \tag{5.2}$$

En este caso el elemento neutro de G se nota con $0=(0,\dots,0)$. Si $g=(g_1,\dots,g_n)\in G$, entonces $-g=(-g_1,\dots,-g_n)$.

5.1.3 Ejemplo. Sea $G=\mathbb{Z}_2\times\mathbb{Z}_2$. La operación sobre G está dada por

+	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

Tabla 5.1: Tabla de multiplicación del grupo $\mathbb{Z}_2\times\mathbb{Z}_2$

Note que G posee la misma estructura que el 4-grupo de Klein. No es isomorfo a $\mathbb{Z}_4$.

5.1.4 Ejemplo. Sea $G=\mathbb{Z}_5\times\mathbb{Z}_2$. La operación sobre G está dada por

+	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$	$(2,0)$	$(2,1)$	$(3,0)$	$(3,1)$	$(4,0)$	$(4,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$	$(2,0)$	$(2,1)$	$(3,0)$	$(3,1)$	$(4,0)$	$(4,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$	$(2,1)$	$(2,0)$	$(3,1)$	$(3,0)$	$(4,1)$	$(4,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(2,0)$	$(2,1)$	$(3,0)$	$(3,1)$	$(4,0)$	$(4,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(2,1)$	$(2,0)$	$(3,1)$	$(3,0)$	$(4,1)$	$(4,0)$	$(0,1)$	$(0,0)$
$(2,0)$	$(2,0)$	$(2,1)$	$(3,0)$	$(3,1)$	$(4,0)$	$(4,1)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(2,1)$	$(2,1)$	$(2,0)$	$(3,1)$	$(3,0)$	$(4,1)$	$(4,0)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(3,0)$	$(3,0)$	$(3,1)$	$(4,0)$	$(4,1)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$	$(2,0)$	$(2,1)$
$(3,1)$	$(3,1)$	$(3,0)$	$(4,1)$	$(4,0)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$	$(2,1)$	$(2,0)$
$(4,0)$	$(4,0)$	$(4,1)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$	$(2,0)$	$(2,1)$	$(3,0)$	$(3,1)$
$(4,1)$	$(4,1)$	$(4,0)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$	$(2,1)$	$(2,0)$	$(3,1)$	$(3,0)$

Tabla 5.2: Tabla de multiplicación del grupo $\mathbb{Z}_5\times\mathbb{Z}_2$

Consideremos ahora todas las potencias de $(1,1)$. Note que

$$\begin{aligned}
1(1,1) &= (1,1)\\
2(1,1) &= (2,0)\\
3(1,1) &= (3,1)\\
4(1,1) &= (4,0)\\
5(1,1) &= (0,1)\\
6(1,1) &= (1,0)\\
7(1,1) &= (2,1)\\
8(1,1) &= (3,0)\\
9(1,1) &= (4,1)\\
10(1,1) &= (0,0).
\end{aligned}$$

Es decir, G es un grupo cíclico generado por $(1,1)$, el cual posee la misma estructura que $\mathbb{Z}_{10}$.

5.1.5 Teorema. Sea $G_1, \ldots, G_n$ grupos. Entonces

(1) $G_1 \times G_2 \cong G_2 \times G_1$

(2) $G_1 \times G_2 \times G_3 \cong G_1 \times (G_2 \times G_3) \cong (G_1 \times G_2) \times G_3$

(3) $G_1 \times \cdots \times G_n \cong G_{\sigma(1)} \times \cdots \times G_{\sigma(n)}$ para todo $\sigma \in \mathrm{Sym}(n)$

(4) $G_1 \times \cdots \times G_n$ es abeliano si y solo si G_j es abeliano para todo $j \in \{1, \ldots, n\}$

(5) $|G_1 \times \cdots \times G_n| = |G_1| \cdots |G_n|$

(6) Sea $g = (g_1, \ldots, g_n) \in \prod_{j=1}^{n} G_j$ tal que cada $\mathrm{ord}(g_j)$ es finito para todo $j \in \{1, \ldots, n\}$. Entonces
$$\mathrm{ord}(g) = \mathrm{mcm}\{\mathrm{ord}(g_j) \mid j = 1, \ldots, n\}.$$

Demostración. (1) Sea $\varphi : G_1 \times G_2 \longrightarrow G_2 \times G_1$ definida por

$$\varphi(g_1, g_2) = (g_2, g_1).$$

Entonces φ es un isomorfismo de grupos.

(2) Sea $\varphi : G_1 \times (G_2 \times G_3) \longrightarrow (G_1 \times G_2) \times G_3$ definida por

$$\varphi(g_1, (g_2, g_3)) = ((g_1, g_2), g_3).$$

Entonces φ es un isomorfismo de grupos.

(3) Sea $\sigma \in \mathrm{Sym}(n)$ y consideremos la función

$$\varphi : G_1 \times \cdots \times G_n \longrightarrow G_{\sigma(1)} \times \cdots \times G_{\sigma(n)}$$

definida por

$$\varphi(g_1, \ldots, g_n) = (g_{\sigma(1)}, \ldots, g_{\sigma(n)}).$$

Entonces φ es un isomorfismo de grupos.

(4) Sean $g_j \in G_j$, para $j = 1, \ldots, n$. Entonces

$$\begin{aligned} G_1 \times \cdots \times G_n \text{ es abeliano} &\Leftrightarrow (g_1, \ldots, g_n)(g_1', \ldots, g_n') = (g_1', \ldots, g_n')(g_1, \ldots, g_n) \\ &\Leftrightarrow (g_1 g_1', \ldots, g_n g_n') = (g_1' g_1, \ldots, g_n' g_n) \\ &\Leftrightarrow g_j g_j' = g_j' g_j \\ &\Leftrightarrow G_j \text{ es abeliano para todo } j \in \{1, \ldots, n\}. \end{aligned}$$

(5) Evidente.

(6) Sean $g := (g_1, \ldots, g_n)$ y $m := \mathrm{ord}(g)$. Entonces

$$g^m = (g_1^n, \ldots, g_n^m) = (1, \ldots, 1)$$

y para todo $j \in \{1, \ldots, n\}$ se verifica que $g_j^m = 1$. Entonces $\mathrm{ord}(g_j) \mid m$ para todo $j \in \{1, \ldots, n\}$. En consecuencia,

$$\mathrm{mcm}\{\mathrm{ord}(g_j) \mid j = 1, \ldots, n\} \mid m.$$

Por otro lado, es claro que

$$m \mid \mathrm{mcm}\{\mathrm{ord}(g_j) \mid j = 1, \ldots, n\},$$

y se tiene la igualdad. □

5.1.6 Teorema. Sean $m, n \in \mathbb{N}$.

(1) Si $\mathrm{mcd}(m, n) = 1$, entonces $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$.

(2) Sean $m_1, \ldots, m_k \in \mathbb{N}$ con $\mathrm{mcd}(m_i, m_j) = 1$ para todo $i \neq j$, $i, j \in \{1, \ldots, n\}$. Entonces $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k} \cong \mathbb{Z}_{m_1 \cdots m_k}$.

(3) Si $n = p_1^{a_1} \cdots p_k^{a_k}$ es la descomposición en factores primos de n, entonces $\mathbb{Z}_{p_1^{a_1}} \times \cdots \times \mathbb{Z}_{p_k^{a_k}} \cong \mathbb{Z}_n$.

DEMOSTRACIÓN. (1) Se verifica sin dificultades que $\text{ord}(1,0) = m$ y $\text{ord}(0,1) = n$. Dado que $\text{mcd}(m,n) = 1$, se tiene que $\text{ord}(1,1) = mn$. Por lo tanto, $\mathbb{Z}_m \times \mathbb{Z}_n$ es cíclico de orden mn y, en consecuencia, isomorfo a $\mathbb{Z}_{mn}$.

(2) Usando (1) e inducción sobre k se tiene la afirmación.

(3) Se sigue de (2). □

5.1.7 Teorema. Sea $G_1, \ldots, G_n$ grupos y para cada $j \in \{1, \ldots, n\}$ definamos

$$\widetilde{G}_j := \{(1, \ldots, 1, \underset{j}{g}, 1, \ldots, 1) \mid g \in G_j\}.$$

Entonces

(1) $G_j \cong \widetilde{G}_j$ para todo $j \in \{1, \ldots, n\}$

(2) $\widetilde{G}_j \trianglelefteq G_1 \times \cdots \times G_n$ para todo $j \in \{1, \ldots, n\}$

(3) $(G_1 \times \cdots \times G_n)/\widetilde{G}_j \cong G_1 \times \cdots \times G_{j-1} \times G_{j+1} \times \cdots \times G_n$.

DEMOSTRACIÓN. (1) Sea $j \in \{1, \ldots, n\}$ y definamos $f_j : G_j \longrightarrow \widetilde{G}_j$ mediante

$$f_j(g) := (1, \ldots, 1, \underset{j}{g}, 1, \ldots, 1).$$

Es claro que f_j es un isomorfismo.

(2) Sea $j \in \{1, \ldots, n\}$ y sean $(1, \ldots, 1, \underset{j}{g}, 1, \ldots, 1) \in \widetilde{G}_j$ y $(g_1, \ldots, g_n) \in G_1 \times \cdots \times G_n$. Entonces

$$(g_1, \ldots, g_n)(1, \ldots, 1, \underset{j}{g}, 1, \ldots, 1)(g_1, \ldots, g_n)^{-1} = (1, \ldots, 1, \underset{j}{g_j g g_j^{-1}}, 1, \ldots, 1) \in \widetilde{G}_j,$$

con lo cual se tiene la normalidad de $\widetilde{G}_j$ para todo $j \in \{1, \ldots, n\}$.

(3) Definamos ahora la función

$$\varphi : G_1 \times \cdots \times G_n \longrightarrow G_1 \times \cdots \times G_{j-1} \times G_{j+1} \times \cdots \times G_n$$

de la siguiente manera:

$$\varphi(g_1, \ldots, g_n) := (g_1, \ldots, g_{j-1}, g_{j+1}, \ldots, g_n).$$

Es claro que φ es un epimorfismo de grupos y

$$\ker(\varphi) = \{(g_1, \ldots, g_n) \mid g_i = 1, \ \forall i \neq j\} = \widetilde{G}_j.$$

El resto se sigue del primer teorema de isomorfía. □

5.2 Producto directo interno

5.2.1 Definición. Sea $J = \{1, \ldots, n\}$ y para cada $j \in J$ sea N_j un subgrupo normal de un grupo G. Decimos que G es el `producto directo interno` de los $\{N_j\}_{j\in J}$ si se verifican las siguientes condiciones:

(1) $G = \langle \bigcup_{j\in J} N_j \rangle$.

(2) $N_i \cap \langle \bigcup_{j\in J\setminus\{i\}} N_j \rangle = 1$.

Cada N_j se denomina un `factor directo` de G. Usamos como antes la notación $\prod_{j=1}^{k} N_j$.

5.2.2 Lema. Sean $N_1, \ldots, N_k$ subgrupos normales de un grupo G. Entonces

(1) $\left\langle \bigcup_{j=1}^{k} N_j \right\rangle = N_1 \cdots N_k = \{n_1 \cdots n_k \mid n_j \in N_j\}$.

(2) $\prod_{j=1}^{k} N_j \trianglelefteq G$.

(3) $\prod_{j=1}^{k} N_j = \prod_{j=1}^{k} N_{\sigma(j)}$ para todo $\sigma \in \mathrm{Sym}(k)$.

Demostración. (1) Procedemos por inducción sobre k.

(a) Si $k = 1$, entonces $\langle N_1 \rangle = N_1$.

(b) Sea $k = 2$. Del teorema 2.1.9 (3) se tiene que $N_1 N_2 \trianglelefteq G$. Es claro que $N_1 N_2 \subseteq \langle N_1 \cup N_2 \rangle$.

Recíprocamente, note que $N_1 \cup N_2 \subseteq N_1 N_2$. Por lo tanto, usando la observación 1.2.15 se sigue que $\langle N_1 \cup N_2 \rangle \subseteq N_1 N_2$.

(c) Como hipótesis de inducción supongamos que

$$\left\langle \bigcup_{j=1}^{k-1} N_j \right\rangle = N_1 \cdots N_{k-1}.$$

Entonces, si definimos $N := \langle \bigcup_{j=1}^{k-1} N_j \rangle$ se tiene que

$$\left\langle \bigcup_{j=1}^{k} N_j \right\rangle = \langle N \cup N_k \rangle.$$

Se verifica sin dificultades que $N \trianglelefteq G$. En efecto para todo $g \in G$

$$\begin{aligned} gNg^{-1} &= gN_1\cdots N_{k-1}g^{-1} \\ &= gN_1g^{-1}gN_2g^{-1}\cdots gN_{k-1}g^{-1} \\ &= N_1\cdots N_{k-1} \\ &= N. \end{aligned}$$

(d) Usando el caso $k = 2$ y la hipótesis de inducción se tiene que

$$\left\langle \bigcup_{j=1}^{k} N_j \right\rangle = \langle N \cup N_k \rangle = NN_k = N_1\cdots N_k.$$

(2) Similar como antes.

(3) La afirmación se sigue del hecho que $\bigcup_{j=1}^{k} N_j = \bigcup_{j=1}^{k} N_{\sigma(j)}$. □

5.2.3 Teorema. Sean $N_1, \ldots, N_k$ subgrupos de un grupo G. Las siguientes afirmaciones son equivalentes:

(1) $G = \prod_{j=1}^{k} N_j$

(2) Se satisfacen las siguientes condiciones:

- (a) Si $g \in N_i$ y $h \in N_j$ con $i \neq j$, entonces $gh = hg$.
- (b) Todo $g \in G$ puede expresarse de manera única en la forma $g = g_1\cdots g_k$, con $g_j \in N_j$.

Demostración. (1) ⇒ (2). Sean $g \in N_i$ y $h \in N_j$ con $i \neq j$. Entonces, dado que $N_i, N_j \trianglelefteq G$, tenemos

$$(ghg^{-1})h^{-1} = g(hg^{-1}h^{-1}) \in N_i \cap N_j.$$

Dado que

$$N_i \cap N_j \subseteq N_i \cap N_1\cdots N_{i-1}N_{i+1}\cdots N_k = 1,$$

se sigue que $ghg^{-1}h^{-1} = 1$. Es decir, $gh = hg$.

Por otro lado, si $g \in G$, entonces por hipótesis se tiene que g puede expresarse en la forma $g = g_1\cdots g_k$, con $g_j \in N_j$. Para demostrar la unicidad supongamos que

$$g = g_1\cdots g_k = h_1\cdots h_k, \quad \text{con} \quad g_j, h_j \in N_j, \quad j = 1, \ldots, k.$$

Para todo $j \in \{1, \ldots, k\}$ se verifica que $h_j^{-1}g_j \in N_j$. Además, usando (a) se tiene que

$$h_j^{-1}g_j = \prod_{\substack{i=1 \\ i\neq j}}^{k} g_i^{-1}h_i \in N_1\cdots N_{j-1}N_{j+1}\cdots N_k = 1.$$

Por lo tanto, $h_j^{-1}g_j = 1$. Es decir, $h_j = g_j$ para todo $j = 1, \ldots, k$.

(2) $\Rightarrow$ (1). Demostramos inicialmente que cada $N_j \trianglelefteq G$. Para ello sean $x \in N_j$ y $g \in G$. Por hipótesis existen $g_j \in N_j$, $j = 1, \ldots, k$ tales que $g = g_1 \cdots g_k$. Usando nuevamente (a) se tiene que

$$gxg^{-1} = (g_1 \cdots g_k)x(g_k^{-1} \cdots g_1^{-1}) = g_j x g_j^{-1} \in N_j.$$

De (b) se sigue que $G = N_1 \cdots N_k$. Por lo tanto, $G = \langle \bigcup_{j=1}^{n} N_j \rangle$, y solo resta demostrar que para todo $j = 1, \ldots, k$

$$N_j \cap N_1 \cdots N_{j-1} N_{j+1} \cdots N_k = 1.$$

Si $g \in N_j \cap N_1 \cdots N_{j-1} N_{j+1} \cdots N_k$, entonces

$$g = 1 \cdots 1 g 1 \ldots 1 = g_1 \cdots g_{j-1} 1 g_{j+1} \cdots g_k,$$

con $g_i \in N_i$ adecuados. De la unicidad en la escritura, garantizada por (b), se tiene que $g = 1$. $\square$

5.2.4 Ejemplos. (1) $(\mathbb{Z}_6, +) = \langle 3 \rangle \times \langle 2 \rangle$

(2) Sea $V = \{1, g, h, gh\}$ el 4-grupo de Klein. Entonces

$$\begin{aligned} V &= \langle g \rangle \times \langle h \rangle \\ &= \langle g \rangle \times \langle gh \rangle \\ &= \langle h \rangle \times \langle gh \rangle. \end{aligned}$$

(3) Todo grupo G puede descomponerse en la suma directa interna trivial $G = G \times 1$. Existen grupos para los cuales esta es la única descomposición posible.

(a) Si $G = \mathrm{Sym}(3)$, entonces los únicos subgrupos normales de G son $1, \langle (123) \rangle$ y G. Entonces tenemos las siguientes opciones:

$$G \times 1, \ \langle (123) \rangle \times 1 \ \text{ y } \ G \times \langle (123) \rangle.$$

Claramente, las dos últimas no satisfacen la definición de producto directo interno.

(b) Si $G = D_8 = \{(1), \alpha, \alpha\beta, \alpha\beta^2, \alpha\beta^3, \beta, \beta^2, \beta^3\}$, donde $\alpha = (24)$ y $\beta = (1234)$ en $\mathrm{Sym}(4)$, entonces se verifica que los únicos subgrupos normales de G son: $1, G, \langle \beta \rangle$, $\langle \beta^2 \rangle$ y dos subgrupos isomorfos al 4-grupo de Klein dados por $U = \{(1), \alpha, \beta^2, \beta^2\alpha\}$ y $V = \{(1), \beta^2, \beta\alpha, \beta^3\alpha\}$. Si G fuese producto directo de dos subgrupos, entonces tendríamos las siguientes posibles opciones:

$$G \times 1, \ \langle \beta \rangle \times \langle \beta^2 \rangle, \ \langle \beta^2 \rangle \times U \ \text{ y } \ \langle \beta^2 \rangle \times V.$$

Dado que

$$\begin{aligned}\langle\beta\rangle \cap \langle\beta^2\rangle &= \{(1), \beta^2\}\\ \langle\beta^2\rangle \cap U &= \{(1), \beta^2\}\\ \langle\beta^2\rangle \cap V &= \{(1), \beta^2\},\end{aligned}$$

se tiene que solo sobrevive la primera opción.

(4) Sea G el grupo aditivo de $\mathrm{Mat}(2, \mathbb{C})$ y denotemos con e_{ij} las matices que tienen un uno en la entrada ij y cero en el resto de posiciones. Sea además

$$N_{ij} = \{\lambda e_{ij} \mid \lambda \in \mathbb{C}\}.$$

Entonces

$$G = N_{11} \oplus N_{12} \oplus N_{21} \oplus N_{22}.$$

A continuación demostramos que al hablar de productos directos no es necesario hacer la distinción entre internos y externos. Concretamente demostramos que, como grupos, estos son isomorfos. Con este resultado queda justificada porqué en ambos casos hemos utilizado la misma notación.

5.2.5 Teorema. Si G es el producto directo interno de los subgrupos normales $N_1, \ldots, N_k$, entonces G es isomorfo al producto directo externo $N_1 \times \cdots \times N_k$.

Demostración. Sea $\varphi : N_1 \times \cdots \times N_k \longrightarrow G$ definida por

$$\varphi((g_1, \ldots, g_k)) \coloneqq g_1 \cdots g_k.$$

Sean $(g_1, \ldots, g_k), (h_1, \ldots, h_k) \in N_1 \times \cdots \times N_k$. Entonces usando el teorema 5.2.3 se sigue que

$$\begin{aligned}\varphi((g_1, \ldots, g_k) \cdot (h_1, \ldots, h_k)) &= \varphi((g_1 h_1, \ldots, g_k h_k))\\ &= g_1 h_1 \cdots g_k h_k\\ &= g_1 \cdots g_k \cdot h_1 \cdots h_k\\ &= \varphi((g_1, \ldots, g_k)) \cdot \varphi((h_1, \ldots, h_k)).\end{aligned}$$

Nuevamente del teorema 5.2.3 se sigue que φ es una biyección. □

En el siguiente teorema demostramos que el producto directo externo de grupos también suministra un producto directo interno de subgrupos.

5.2.6 Teorema. Sea $G_1, \ldots, G_k$ grupos y $G = \prod_{j=1}^{k} G_j$. Entonces G es el producto directo interno de los subgrupos normales

$$N_i \coloneqq \{(1, \ldots, 1, g, 1, \ldots, 1) \mid g \in G_i\} \cong G_i, \quad \text{para} \quad i = 1, \ldots, k.$$

DEMOSTRACIÓN. Se deja como ejercicio. □

5.2.7 Lema. Sea $G_1, \ldots, G_k$ y $H_1, \ldots, H_k$ grupos y $\varphi_j : G_j \to H_j$ isomorfismos de grupos para $j = 1, \ldots, k$. Entonces

$$\varphi : G_1 \times \cdots \times G_k \longrightarrow H_1 \times \cdots \times H_k$$

definida por

$$\varphi((g_1, \ldots, g_k)) \coloneqq (\varphi_1(g_1), \ldots, \varphi_k(g_k))$$

es un isomorfismo de grupos.

DEMOSTRACIÓN. Se deja como ejercicio. □

5.2.8 Teorema. Sea G y H grupos finitos cíclicos. Entonces $G \times H$ es un grupo cíclico si y solo si $\text{mcd}(|G|, |H|) = 1$.

DEMOSTRACIÓN. Sean $|G| = m$ y $|H| = n$.

(1) Supongamos que $G = \langle g \rangle$, $H = \langle h \rangle$ y $\text{mcd}(m, n) = 1$. Dado que

$$\text{ord}((g, h)) = \text{mcm}(m, n) = mn = |G \times H|,$$

se sigue que $G \times H = \langle (g, h) \rangle$.

(2) Supongamos que $G \times H = \langle (g, h) \rangle$. Entonces se sigue que $G = \langle g \rangle$ y $H = \langle h \rangle$. Esto significa que $\text{ord}(g) = m$ y $\text{ord}(h) = n$. Dado que $|G \times H| = mn$, se sigue que

$$\text{ord}((g, h)) = mn.$$

Por otro lado, también se tiene que

$$\text{ord}((g, h)) = \text{mcm}(m, n).$$

De la teoría básica de números se tiene que

$$\text{mcd}(m, n)\text{mcm}(m, n) = mn.$$

Por lo tanto,

$$\text{mcd}(m, n) = 1$$

y se tiene la afirmación. □

5.3 Producto directo externo - caso infinito

5.3.1 Definición. Sean $\{G_j\}_{j\in J}$ una familia de grupos y G el conjunto definido por

$$G := \Big\{ f \;\Big|\; f : J \longrightarrow \bigcup_{j\in J} G_j \text{ con } \; f(j) \in G_j \Big\}.$$

Definamos sobre G la siguiente multiplicación:

$$(f \cdot g)(j) := f(j) \cdot g(j) \text{ para todo } j \in J \ . \tag{5.3}$$

La asociatividad de esta multiplicación es evidente. Si para cada $j \in J$ notamos con 1 el elemento identidad de G_j, entonces $e(j) = 1$ es el elemento identidad de G. Si $f \in G$, entonces f^{-1} es la función $f^{-1}(j) = f(j)^{-1}$. Entonces $(G, \cdot)$ es un grupo, el cual se denomina `producto directo externo no restringido` o `producto cartesiano` de los grupos $\{G_j\}_{j\in J}$ y se nota con

$$G = \prod_{j\in J} G_j.$$

5.3.2 Ejemplo. Si $J = \mathbb{N}$, y para cada $j \in \mathbb{N}$ se tiene que G_j es el grupo aditivo de un anillo R, entonces el producto cartesiano $\prod_{j\in J} G_j$ es isomorfo al grupo aditivo de las series de potencia con coeficientes en R. En efecto, si definimos

$$f \longmapsto \sum_{j=0}^{\infty} f(j)x^j$$

se verifica que esta función es un isomorfismo, la cual identifica cada $f \in \prod_{j\in J} G_j$ con la sucesión de sus imágenes $(f(1), \ldots, f(n), \ldots)$.

5.3.3 Observaciones. (1) Si J es finito, entonces $\prod_{j\in J} G_j \cong G_1 \times \cdots \times G_n$. En efecto, la función

$$f \longmapsto (f(1), \ldots, f(n))$$

es un isomorfismo de grupos.

(2) Las `proyecciones canónicas` π_j se definen de la siguiente manera:

$$\pi_j : \prod_{j\in J} G_j \longrightarrow \; G_j,$$

$$\pi_j(f) = f(j).$$

O equivalentemente,

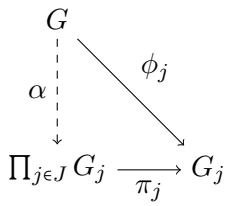
$$\pi_j(f) = f_j,$$

donde $f_j = f(j)$. Se verifica sin dificultades que cada π_j es un epimorfismo de grupos.

El siguiente teorema demuestra que el producto cartesiano $\prod_{j\in J} G_j$ satisface una propiedad universal.

5.3.4 Teorema. Sean $\{G_j\}_{j\in J}$ una familia de grupos y $\{\pi_j\}_{j\in J}$ las proyecciones canónicas. Entonces

(1) Para todo grupo G con homomorfismos $\phi_j : G \longrightarrow G_j$, $j \in J$ existe un único homomorfismo $\alpha : G \longrightarrow \prod_{j\in J} G_j$ tal que para todo $j \in J$ se verifica $\pi_j \circ \alpha = \phi_j$. Es decir, para todo $j \in J$ el siguiente diagrama es conmutativo:



(2) Si H es otro grupo con homomorfismos $\phi'_j : H \longrightarrow G_j$, $j \in J$ que satisface (1), entonces H es isomorfo al producto cartesiano.

Demostración. (1) `Existencia de` α. Definamos $\alpha : G \longrightarrow \prod_{j\in J} G_j$ de la siguiente manera: para cada $g \in G$ definimos

$$\alpha(g) : J \longrightarrow \bigcup_{j\in J} G_j \tag{5.4}$$

mediante

$$\alpha(g)(j) \coloneqq \phi_j(g).$$

Sean $g_1, g_2 \in G$. Entonces

$$\begin{aligned}\alpha(g_1g_2)(j) &\coloneqq \phi_j(g_1g_2)\\ &= \phi_j(g_1)\phi_j(g_2)\\ &= \alpha(g_1)(j)\alpha(g_2)(j)\\ &= \alpha(g_1)\alpha(g_2)(j)\end{aligned}$$

para todo $j \in J$. Por lo tanto, α es un homomorfismo de grupos.

Por otro lado, para todo $j \in J$ y para todo $g \in G$ se tiene que

$$(\pi_j \circ \alpha)(g) = \pi_j(\alpha(g)) = \alpha(g)(j) = \phi_j(g),$$

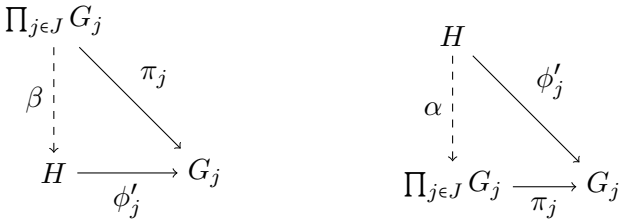
con lo cual se sigue que el diagrama de arriba es conmutativo.

`Unicidad de` α. Sea φ otro homomorfismo de G en $\prod_{j\in J} G_j$ que hace conmutativos los diagramas. Entonces para todo $g \in G$ se verifica que

$$\alpha(g)(j) = \pi_j(\alpha(g)) = (\pi_j \circ \alpha)(g) = \phi_j(g) = (\pi_j \circ \varphi)(g) = \pi_j(\varphi(g)) = \varphi(g)(j).$$

En consecuencia, $\varphi = \alpha$.

(2) Dado que tanto H como el producto cartesiano $\prod_{j\in J} G_j$ satisfacen la propiedad (1) para todo $j \in J$ se verifica que los siguientes diagramas conmutan:



Es decir, $\phi'_j \circ \beta = \pi_j$ y $\pi_j \circ \alpha = \phi'_j$. Entonces para todo $j \in J$

$$\pi_j \circ (\alpha \circ \beta) = \pi_j$$

y

$$\phi'_j \circ (\beta \circ \alpha) = \phi'_j,$$

Dado que

$$\pi_j \circ I_{\prod_{j\in J} G_j} = \pi_j$$

y

$$\phi'_j \circ I_H = \phi'_j,$$

la unicidad de la función en (1) garantiza que $\alpha \circ \beta = I_{\prod_{j\in J} G_j}$ y $\beta \circ \alpha = I_H$, con lo cual se tiene la isomorfía entre H y el producto cartesiano. □

5.3.5 Observación. El isomorfismo α entre H y $\prod_{j\in J} G_j$ garantizado por el teorema anterior puede tenerse de manera explícita.

Note que dado $h \in H$, definimos $f(j) := \phi'_j(h)$. Entonces

$$\begin{aligned} f(j) &= \phi'_j(h) \\ &= \phi'_j \circ (\beta \circ \alpha)(h) \\ &= \pi_j \circ \alpha(h) \\ &= \alpha(h)(j). \end{aligned}$$

Entonces $\alpha(h) = f$.

5.4 Suma directa externa - caso infinito

5.4.1 Definición. Sea $\{G_j\}_{j\in J}$ una familia de grupos. Si $f \in \prod_{j\in J} G_j$, entonces se define el `soporte` de f, notado $\text{sop}(f)$, como el conjunto de índices $j \in J$ tales que $f(j) \neq 1$. Esto es,

$$\text{sop}(f) := \{j \in J \mid f(j) \neq 1\}.$$

5.4.2 Teorema. Sea $\{G_j\}_{j\in J}$ una familia de grupos. Entonces el subconjunto de $\prod_{j\in J} G_j$ formado por todas las funciones con soporte finito es un subgrupo normal del producto cartesiano $\prod_{j\in J} G_j$, el cual se denomina `suma directa externa` de los $\{G_j\}_{j\in J}$ o `coproducto externo` de los $\{G_j\}_{j\in J}$y se nota con

$$\bigoplus_{j\in J} G_j.$$

Demostración. Dado que el elemento identidad del producto cartesiano $\prod_{j\in J} G_j$ tiene soporte vacío, se tiene que $\bigoplus_{j\in J} G_j \neq \varnothing$.

Sean ahora $f, g \in \bigoplus_{j\in J} G_j$ con $\text{sop}(f) = I$, $\text{sop}(g) = K$. Entonces $\text{sop}(f^{-1}) = \text{sop}(f)$ y $\text{sop}(fg) \subset I \cup K$, el cual es claramente finito. Esto demuestra que $\bigoplus_{j\in J} G_j \leq \prod_{j\in J} G_j$.

Para la normalidad, sean $f \in \prod_{j\in J} G_j$ y $g \in \bigoplus_{j\in J} G_j$. Entonces $\text{sop}(f^{-1}gf) = \text{sop}(g)$. Por lo tanto, $f^{-1}gf \in \bigoplus_{j\in J} G_j$. □

5.4.3 Ejemplo. Si $J = \mathbb{N}$, y para cada $j \in \mathbb{N}$ se tiene que G_j es el grupo aditivo de un anillo R, entonces la suma directa externa $\bigoplus_{j\in J} G_j$ es isomorfo al grupo aditivo de los polinomios con coeficientes en R. En efecto, si definimos

$$f \longmapsto \sum_{j=0}^{|\text{sop}(f)|} f(j)x^j$$

se verifica que esta función es un isomorfismo, la cual identifica cada $f \in \prod_{j\in J} G_j$ con la sucesión de sus imágenes $(f(1), \ldots, f(n), \ldots)$.

5.4.4 Observación. Si $J = \{1, \ldots, n\}$, entonces $\prod_{j\in J} G_j \cong \bigoplus_{j\in J} G_j \cong G_1 \times \cdots \times G_n$.

5.4.5 Lema. Sea $\{G_j\}_{j\in J}$ una familia de grupos. Para cada $j \in J$ definamos

$$\mu_j : G_j \longrightarrow \bigoplus_{j\in J} G_j$$

mediante $\mu_j(g) := f$, donde

$$f : J \longrightarrow \bigcup_{j\in J} G_j$$

está definida por

$$f(k) := \begin{cases} g & \text{si } \ k = j \\ 1 & \text{si } \ k \neq j. \end{cases}$$

Entonces para cada $j \in J$ se tiene que μ_j es un monomorfismo de grupos, el cual se denomina `inyección canónica` de la j-ésima componente.

Demostración. Utilizando la notación del delta de Kronecker tenemos

$$\mu_j(g)(k) = g^{\delta_{jk}}.$$

Entonces para todo $j, k \in J$ y todo $g, h \in G$

$$\begin{aligned} \mu_j(gh)(k) &= (gh)^{\delta_{jk}} \\ &= g^{\delta_{jk}} h^{\delta_{jk}} \\ &= \mu_j(g)(k)\mu_j(h)(k) \\ &= (\mu_j(g)\mu_j(h))(k). \end{aligned}$$

Esto demuestra que cada μ_j es un homomorfismo de grupos. La inyectividad es clara. □

5.4.6 Observaciones. Es inmediato verificar que

(1) $\pi_j \circ \mu_j = I_{G_j}$ para todo $j \in J$.

(2) $\mu_i(g_i)\mu_j(g_j) = \mu_j(g_j)\mu_i(g_i)$ para todo $i, j \in J$ con $i \neq j$, $g_i \in G_i$ y $g_j \in G_j$.

(3) $\prod_{j \in J} \mu_j(\pi_j(g)) = g$ para todo $g \in \bigoplus_{j \in J} G_j$.

5.4.7 Teorema. Sea H un grupo abeliano y para cada $j \in J$ sea $\phi_j : G_j \longrightarrow H$ un homomorfismo de grupos. Entonces existe un único homomorfismo de grupos

$$\phi : \bigoplus_{j \in J} G_j \longrightarrow H$$

tal que $\phi \circ \mu_j = \phi_j$.

Demostración. (1) `Existencia.` Sea $f \in \bigoplus_{j \in J} G_j$ con soporte finito I. Si $i \in I$, entonces $f(i) \in G_i$ y $\phi_i(f(i)) \in H$. Definamos entonces

$$\varphi(f) := \prod_{i \in I} \phi_i(f(i))$$

y demostremos que φ es un homomorfismo. Sea además $g \in \bigoplus_{j\in J} G_j$ y sin perder generalidad supongamos que $\varphi(g) := \prod_{i\in I} \phi_i(g(i))$. Note que solo es necesario agregar un número finito de unos, si fuese necesario. Entonces, dado que H es abeliano, tenemos

$$\begin{aligned}
\varphi(fg) &= \prod_{i\in I} \phi_i(fg(i)) \\
&= \prod_{i\in I} \phi_i(f(i)g(i)) \\
&= \prod_{i\in I} \phi_i(f(i))\phi_i(g(i)) \\
&= \prod_{i\in I} \phi_i(f(i)) \prod_{i\in I} \phi_i(g(i)) \\
&= \varphi(f)\varphi(g).
\end{aligned}$$

Finalmente, dado que para todo $j \in J$ el soporte de μ_j es $\{j\}$, se tiene que

$$(\phi \circ \mu_j)(g) = \phi_j(\mu_j(g)(j)) = \phi_j(g),$$

para todo $g \in G_j$. En consecuencia, $\phi \circ \mu_j = \phi_j$ para todo $j \in J$.

(2) `Unicidad.` Supongamos que φ y ψ satisfacen tales condiciones. Sea $f \in \bigoplus_{j\in J} G_j$ con $\operatorname{sop}(f) = \{j_1, \ldots, j_n\}$. Entonces

$$\varphi(f) = \varphi\Big(\prod_{i=1}^{n} f_{j_i}\Big) = \prod_{i=1}^{n} \varphi(f_{j_i}) = \prod_{i=1}^{n} \varphi(\mu_{j_i}(f(j_i))) = \prod_{i=1}^{n} \phi_{j_i}(f(j_i)).$$

Por otro lado,

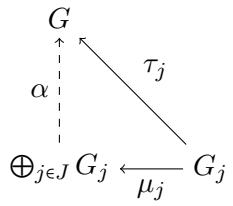
$$\psi(f) = \psi\Big(\prod_{i=1}^{n} f_{j_i}\Big) = \prod_{i=1}^{n} \psi(f_{j_i}) = \prod_{i=1}^{n} \psi(\mu_{j_i}(f(j_i))) = \prod_{i=1}^{n} \phi_{j_i}(f(j_i)),$$

con lo cual se tiene que $\varphi = \psi$. □

La suma directa externa de grupos también satisface una propiedad universal.

5.4.8 Teorema. Sean $\{G_j\}_{j\in J}$ una familia de grupos abelianos, $\bigoplus_{j\in J} G_j$ su suma directa externa y $\mu_j : G_j \longrightarrow \bigoplus_{j\in J} G_j$ sus inyecciones canónicas. Entonces:

(1) Para todo grupo G con homomorfismos $\tau_j : G_j \longrightarrow \bigoplus_{j\in I} G_j$ existe un único homomorfismo $\alpha : \bigoplus_{j\in J} G_j \longrightarrow G$ tal que para todo $j \in J$ se verifica $\alpha \circ \mu_j = \tau_j$. Es decir, para todo $j \in J$ el siguiente diagrama es conmutativo:



(2) Si H es otro grupo con homomorfismos $\mu'_j : G_j \longrightarrow H$, $j \in J$ que satisface (1), entonces H es isomorfo a la suma directa externa.

DEMOSTRACIÓN. (1) Para $g \in \bigoplus_{j\in J} G_j$, sea $g_j := g(j)$, para $j \in J$ y definamos $\alpha(1) := 1$ y para $g \neq 1$ sea α definida por

$$\alpha(g) := \prod_{j\in \mathrm{sop}(g)} \tau_j(g_j).$$

(a) α `es un homomorfismo.` Sean $f, g \in \bigoplus_{j\in J} G_j$.

Caso 1. Si $f = 1$ o $g = 1$, entonces claramente $\alpha(fg) = \alpha(f)\alpha(g)$.

Caso 2. Si $f, g \neq 1$ y $fg = 1$, entonces $g_j = f_j^{-1}$ para todo $j \in J$ y se tiene que

$$\alpha(fg) = 1 = \prod_{j\in \mathrm{sop}(f)} \tau_j(f_j) \prod_{j\in \mathrm{sop}(g)} \tau_j(g_j) = \alpha(f)\alpha(g).$$

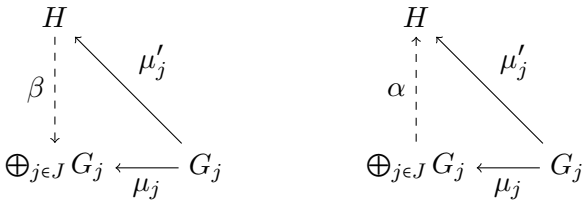
Caso 3. Si $f, g \neq 1$ y $fg \neq 1$, entonces definamos $h := fg$, y dado que $\mathrm{sop}(h) \subseteq \mathrm{sop}(f) \cup \mathrm{sup}(g)$, se tiene que

$$\begin{aligned}
\alpha(fg) &= \prod_{j\in \mathrm{sop}(h)} \tau_j(h_j) \\
&= \prod_{j\in \mathrm{sop}(f)\cup \mathrm{sup}(g)} \tau_j(h_j) \\
&= \prod_{j\in \mathrm{sop}(f)\cup \mathrm{sup}(g)} \tau_j(f_j g_j) \\
&= \prod_{j\in \mathrm{sop}(f)\cup \mathrm{sup}(g)} \tau_j(f_j) \prod_{j\in \mathrm{sop}(f)\cup \mathrm{sup}(g)} \tau_j(g_j) \\
&= \prod_{j\in \mathrm{sop}(f)} \tau_j(f_j) \prod_{j\in \mathrm{sup}(g)} \tau_j(g_j) \\
&= \alpha(f)\alpha(g).
\end{aligned}$$

(b) `Unicidad de` α. Sea $\alpha' : \bigoplus_{j\in J} G_j \longrightarrow G$ otro homomorfismo tal que para todo $j \in J$ se verifica $\alpha' \circ \mu_j = \tau_j$ y sea $f \in \bigoplus_{j\in J} G_j$ cualquiera. Si $f = 1$, entonces claramente $\alpha(f) = \alpha'(f) = 1$. Supongamos entonces que $f \neq 1$. En consecuencia,

$$\begin{aligned}
\alpha(f) &= \prod_{j\in \mathrm{sop}(f)} \tau_j(f_j) \\
&= \prod_{j\in \mathrm{sop}(f)} (\alpha' \circ \mu_j)(f_j) \\
&= \alpha'\Big(\prod_{j\in \mathrm{sop}(f)} \mu_j(f_j) \Big) \\
&= \alpha'(f).
\end{aligned}$$

(2) Por las propiedades que satisfacen H y la suma directa externa $\bigoplus_{j\in J} G_j$, para todo $j \in J$ se verifica que los siguientes diagramas conmutan:

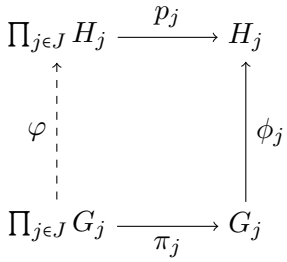


Es decir, $\beta \circ \mu'_j = \mu_j$ y $\alpha \circ \mu_j = \mu'_j$ para todo $j \in J$. Similar como se vio en el producto directo externo, de la unicidad se sigue que $\alpha \circ \beta = I_H$ y $\beta \circ \alpha = I_{\bigoplus_{j\in J} G_j}$. Por lo tanto, H y $\bigoplus_{j\in J} G_j$ son isomorfos. □

5.4.9 Definición. Sean $(G_j)_{j\in J}$ y $(H)_{j\in J}$ dos familias de grupos y sea $(\phi_j)_{j\in J}$ una familia de homomorfismos, donde $\phi_j : G_j \longrightarrow H_j$ para todo $j \in J$. Denotemos con π_j y p_j las proyecciones canónicas de los respectivos productos directos de las familias de grupos. Entonces el único homomorfismo

$$\varphi : \prod_{j\in J} G_j \longrightarrow \prod_{j\in J} H_j$$

tal que $p_j \circ \varphi = \phi_j \circ \pi_j$ se denomina `producto directo` de los ϕ_j y se nota con $\prod_{j\in J} \phi_j$.



5.4.10 Teorema. Sean $(G_j)_{j\in J}$ y $(H)_{j\in J}$ dos familias de grupos y sea $(\phi_j)_{j\in J}$ una familia de homomorfismos, donde $\phi_j : G_j \longrightarrow H_j$ para todo $j \in J$. Entonces

(1) $\varphi(\bigoplus_{j\in J} G_j) \subseteq \bigoplus_{j\in J} H_j$.

(2) $\ker(\prod_{j\in J} \phi_j) = \prod_{j\in J} \ker(\phi_j)$.

(3) φ es un monomorfismo si y solo si ϕ_j es un monomorfismo para todo $j \in J$.

(4) $\mathrm{Im}(\prod_{j\in J}\phi_j) = \prod_{j\in J}\mathrm{Im}(\phi_j)$.

(5) φ es un epimorfismo si y solo si ϕ_j es un epimorfismo para todo $j \in J$.

DEMOSTRACIÓN. Note inicialmente que para todo $i \in J$ y todo $f \in \prod_{j\in J} G_j$ se verifica que

$$\begin{aligned}\varphi(f)(i) &= p_i(\varphi(f))\\ &= (p_i \circ \varphi)(f)\\ &= (\phi_i \circ \pi_i)(f)\\ &= \phi_i(\pi_i(f))\\ &= \phi_i(f(i)).\end{aligned}$$

(1) Esta afirmación se sigue del hecho que $\mathrm{sop}(\varphi(f)) \subseteq \mathrm{sop}(f)$. Entonces, si f tiene soporte finito, $\varphi(f)$ también lo tiene.

(2) Sea $f \in \prod_{j\in J} G_j$. Entonces

$$\begin{aligned}f \in \ker(\varphi) &\iff \varphi(f) = 0\\ &\iff \varphi(f)(i) = 0, \quad \forall i \in J\\ &\iff \phi_i(f(i)) = 0, \quad \forall i \in J\\ &\iff f(i) \in \ker(\phi_i), \quad \forall i \in J\\ &\iff f \in \prod_{j\in J} \ker(\phi_j).\end{aligned}$$

(3) Se sigue de (2).

(4) Sea $g \in \prod_{j\in J} H_j$. Entonces

$$\begin{aligned}g \in \mathrm{Im}(\varphi) &\iff \text{existe} f \in \prod_{j\in J} G_j \text{ tal que } g = \varphi(f),\\ &\iff \text{existe} f \in \prod_{j\in J} G_j \text{ tal que } g(i) = \varphi(f)(i), \quad \forall i \in J\\ &\iff \text{existe} f \in \prod_{j\in J} G_j \text{ tal que } g(i) = \phi_i(f(i)), \quad \forall i \in J\\ &\iff g(i) \in \mathrm{Im}(\phi_i), \quad \forall i \in J\\ &\iff g \in \prod_{j\in J} \mathrm{Im}(\phi_j).\end{aligned}$$

(5) Si para cada $j \in J$ se tiene que ϕ_j es un epimorfismo, entonces $\mathrm{Im}(\phi_j) = H_j$ y se tiene que

$$\mathrm{Im}(\varphi) = \prod_{j\in J} \mathrm{Im}(\phi_j) = \prod_{j\in J} H_j.$$

Recíprocamente, supongamos que $\mathrm{Im}(\varphi) = \prod_{j\in J} H_j$. Para demostrar la sobreyectividad de cada ϕ_i, sea $h \in H_i$ y definamos $g \in \prod_{j\in J} H_j$ mediante $g(j) = h^{\delta_{ij}}$.

La sobreyectividad de φ garantiza la existencia de $f \in \prod_{j\in J} G_j$ tal que $\varphi(f) = g$. Sea ahora $x := f(i) \in G_i$. Entonces

$$\begin{aligned}\phi_i(x) &= \phi_i(f(i)) \\ &= \varphi(f)(i) \\ &= g(i) \\ &= h. \quad \square\end{aligned}$$

5.4.11 Teorema. Sea $(G_j)_{j\in J}$ una familia de grupos y para todo $j \in J$ sea $N_j \trianglelefteq G_j$. Entonces

(1) $\prod_{j\in J} N_j \trianglelefteq \prod_{j\in J} G_j$

(2) $\prod_{j\in J} G_j / \prod_{j\in J} N_j \cong \prod_{j\in J} G_j/N_j$

(3) $\bigoplus_{j\in J} N_j \trianglelefteq \bigoplus_{j\in J} G_j$

(4) $\bigoplus_{j\in J} G_j / \bigoplus_{j\in J} N_j \cong \bigoplus_{j\in J} G_j/N_j$.

Demostración. Se deja como ejercicio. $\square$

5.5 Producto semidirecto

A lo largo de esta sección G denota siempre un grupo.

5.5.1 Definición. Sean $N \trianglelefteq G$ y $U \leq G$. Decimos que G es el `producto semidirecto interno` de N con U si se verifica que $G = NU$ y $U \cap N = 1$. Para efectos de notación escribimos $G = N \rtimes U$.

5.5.2 Ejemplo. Sea $G = \mathrm{Sym}(3)$, $N = \langle(123)\rangle$ y $U = \langle(12)\rangle$. Sabemos que $N \trianglelefteq G$, $G = NU$ y $N \cap U = 1$. Entonces $\mathrm{Sym}(3) = N \rtimes U$.

5.5.3 Ejemplo. Sea $G = \mathrm{Alt}(4)$, $N = \{(1), (12)(34), (13)(24), (14)(23)\}$ y $U = \langle(123)\rangle$ es un subgrupo de orden 3. Sabemos que $N \trianglelefteq G$, $G = NU$, y dado que $\mathrm{mcd}(|N|, |U|) = 1$, se tiene que $N \cap U = 1$. Entonces $\mathrm{Alt}(4) = N \rtimes U$.

5.5.4 Definición. Sea G y H grupos. Si existe un homomorfismo $\alpha : H \longrightarrow \mathrm{Aut}(G)$, entonces decimos que H `opera sobre` G, vía α. Es decir, cada $h \in H$ tiene asociado un automorfismo de G, digamos $\alpha(h)$.

5.5.5 Teorema. Sea H un grupo que opera sobre G, vía α. Sobre el conjunto $G \times H$ definamos la siguiente operación:

$$(g_1, h_1) \cdot (g_2, h_2) \coloneqq (g_1\alpha(h_1)(g_2), h_1h_2),$$

entonces $G \times H$ adquiere la estructura de grupo, el cual llamamos producto `semidirecto externo` de G con H, con respecto a α y lo notamos con $G \rtimes_\alpha H$.

Demostración. Demostramos inicialmente la asociatividad de la multiplicación. Sean $g_1, g_2, g_3 \in G$ y $h_1, h_2, h_3 \in H$. Entonces

$$\begin{aligned}
(g_1, h_1) \cdot ((g_2, h_2) \cdot (g_3, h_3)) &= (g_1, h_1) \cdot (g_2\alpha(h_2)(g_3), h_2h_3) \\
&= (g_1\alpha(h_1)(g_2\alpha(h_2)(g_3)), h_1h_2h_3) \\
&= (g_1\alpha(h_1)(g_2)\alpha(h_1)(\alpha(h_2)(g_3)), h_1h_2h_3) \\
&= (g_1\alpha(h_1)(g_2)\alpha(h_1h_2)(g_3), h_1h_2h_3) \\
&= (g_1\alpha(h_1)(g_2), h_1h_2) \cdot (g_3, h_3) \\
&= ((g_1, h_1) \cdot (g_2, h_2)) \cdot (g_3, h_3).
\end{aligned}$$

Se verifica que $(1, 1)$ es el módulo de $G \rtimes_\alpha H$. En efecto,

$$(1, 1) \cdot (g_2, h_2) \coloneqq (1\alpha(1)(g_2), 1h_2) = (1g_2, 1h_2) = (g_2, h_2).$$

Además, para $g \in G$ y $h \in H$

$$\begin{aligned}
(g, h) \cdot (\alpha(h^{-1})(g^{-1}), h^{-1}) &= (g\alpha(h)(\alpha(h^{-1})(g^{-1})), hh^{-1}) \\
&= (g\alpha(hh^{-1})(g^{-1}), hh^{-1}) \\
&= (g\alpha(1)(g^{-1}), hh^{-1}) \\
&= (gg^{-1}, hh^{-1}) \\
&= (1, 1).
\end{aligned}$$

Por lo tanto, $(g, h)^{-1} = (\alpha(h^{-1})(g^{-1}), h^{-1})$. □

5.5.6 Observación. Note que si α es el homomorfismo trivial. Es decir, para todo $h \in H$ se verifica que $\alpha(h)$ es la función idéntica sobre G, entonces $G \rtimes_\alpha H = G \times H$.

5.5.7 Ejemplo. Sea $\alpha : \mathbb{Z}_2 \longrightarrow \mathrm{Aut}(\mathbb{Z}_4)$ un homomorfismo. En el capítulo anterior se demostró que $\mathrm{Aut}(\mathbb{Z}_4) = \{I, \alpha_3\}$, donde I denota la función identidad sobre $\mathbb{Z}_4$ y $\alpha_3(x) = 3x \bmod 4$ (ver ejemplo 4.4.3). Diferenciamos las diferentes posibilidades.

- De la observación anterior tenemos que si $\alpha(1) = I$, entonces α es el homomorfismo trivial y el producto semidirecto correspondiente es el grupo $\mathbb{Z}_4 \times \mathbb{Z}_2$.
- Si $\alpha(1) = \alpha_3$, entonces $\alpha(0) = I$. Usando el teorema anterior se tiene la siguiente tabla de multiplicación para $G \rtimes_\alpha H$:

$\cdot$	$(0,0)$	$(1,0)$	$(2,0)$	$(3,0)$	$(0,1)$	$(1,1)$	$(2,1)$	$(3,1)$
$(0,0)$	$(0,0)$	$(1,0)$	$(2,0)$	$(3,0)$	$(0,1)$	$(1,1)$	$(2,1)$	$(3,1)$
$(1,0)$	$(1,0)$	$(2,0)$	$(3,0)$	$(0,0)$	$(1,1)$	$(2,1)$	$(3,1)$	$(0,1)$
$(2,0)$	$(2,0)$	$(3,0)$	$(0,0)$	$(1,0)$	$(2,1)$	$(3,1)$	$(0,1)$	$(1,1)$
$(3,0)$	$(3,0)$	$(0,0)$	$(1,0)$	$(2,0)$	$(3,1)$	$(0,1)$	$(1,1)$	$(2,1)$
$(0,1)$	$(0,1)$	$(3,1)$	$(2,1)$	$(1,1)$	$(0,0)$	$(3,0)$	$(2,0)$	$(1,0)$
$(1,1)$	$(1,1)$	$(0,1)$	$(3,1)$	$(2,1)$	$(1,0)$	$(0,0)$	$(3,0)$	$(2,0)$
$(2,1)$	$(2,1)$	$(1,1)$	$(0,1)$	$(3,1)$	$(2,0)$	$(1,0)$	$(0,0)$	$(3,0)$
$(3,1)$	$(3,1)$	$(2,1)$	$(1,1)$	$(0,1)$	$(3,0)$	$(2,0)$	$(1,0)$	$(0,0)$

Tabla 5.3: Tabla de multiplicación del grupo $\mathbb{Z}_4 \rtimes_\alpha \mathbb{Z}_2$

5.5.8 Ejemplo. Sea $G = \langle g \rangle$ con $\mathrm{ord}(g) = n$ y $H = \langle h \rangle$ con $\mathrm{ord}(h) = 2$. Definamos $\alpha : H \longrightarrow \mathrm{Aut}(G)$ de la siguiente manera: $\alpha(1) = I$, la función identidad sobre G y $\alpha(h)(g) = g^{-1}$ para todo $g \in G$. Se deja como ejercicio demostrar que el producto semidirecto de G con H es isomorfo al `grupo diédrico` de orden n.

5.5.9 Teorema. Sea H un grupo que opera sobre G, vía α. Si definimos en $G \rtimes_\alpha H$ los conjuntos $\overline{G} = \{(g,1) \mid g \in G\}$ y $\overline{H} = \{(1,h) \mid h \in H\}$, entonces

(1) $G \cong \overline{G} \trianglelefteq G \rtimes_\alpha H$.

(2) $H \cong \overline{H} \leq G \rtimes_\alpha H$.

(3) $G \rtimes_\alpha H = \overline{G}\,\overline{H}$ y $\overline{G} \cap \overline{H} = 1$.

Es decir, $G \rtimes_\alpha H$ es producto semidirecto interno de $\overline{G}$ con $\overline{H}$ y tenemos nuevamente la situación

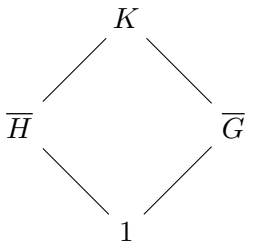


Figura 5.1: Producto semidirecto interno

DEMOSTRACIÓN. (1) Sea $\varphi : G \longrightarrow \overline{G}$ definida por $\varphi(g) := (g, 1)$. Para todo $g, g' \in G$ tenemos:

$$\begin{aligned}\varphi(gg') &= (gg', 1)\\ &= (g\alpha(1)(g'), 1)\\ &= (g, 1) \cdot (g', 1)\\ &= \varphi(g)\varphi(g').\end{aligned}$$

Es claro que φ es biyectiva.

Demostramos ahora que $\overline{G} \trianglelefteq G \rtimes_\alpha H$. Para ello consideremos inicialmente el siguiente resultado:

$$\begin{aligned}(g, 1)^{(1,h)} &= (1, h)^{-1} \cdot (g, 1) \cdot (1, h)\\ &= (1, h^{-1}) \cdot (g, 1) \cdot (1, h)\\ &= (1, h^{-1}) \cdot (g, h)\\ &= (1\alpha(h^{-1})(g), h^{-1}h)\\ &= (\alpha(h^{-1})(g), 1) \in \overline{G}.\end{aligned}$$

Sean ahora $(g_1, 1) \in \overline{G}$ y sea $(g_2, h) \in G \rtimes_\alpha H$ cualquiera. Entonces

$$\begin{aligned}(g_1, 1)^{(g_2,h)} &= (g_2, h)^{-1} \cdot (g_1, 1) \cdot (g_2, h)\\ &= (1, h^{-1}) \cdot (g_2^{-1}, 1) \cdot (g_1, 1) \cdot (g_2, 1) \cdot (1, h)\\ &= (1, h^{-1}) \cdot (g_2^{-1}g_1g_2, 1) \cdot (1, h) \in \overline{G}.\end{aligned}$$

(2) Sea $\psi : H \longrightarrow \overline{H}$ definida por $\psi(h) := (1, h)$. Es claro que ψ es biyectiva. Además para

todo $h, h' \in H$

$$\begin{aligned}\psi(hh') &= (1, hh') \\ &= (1\alpha(h)(1), hh') \\ &= (1, h) \cdot (1, h') \\ &= \psi(h)\psi(h').\end{aligned}$$

(3) Es inmediato. □

5.5.10 Teorema. Sea G un grupo, $N \trianglelefteq G$ y $U \leq G$. Si G es el producto semidirecto interno de N con U, es decir, $G = NU$ y $U \cap N = 1$, entonces G es isomorfo al producto semidirecto externo $N \rtimes_\alpha U$, donde

$$\alpha : U \longrightarrow \mathrm{Aut}(N)$$

está definida por $\alpha(u)(n) := unu^{-1}$ para todo $u \in U$ y $n \in N$.

Demostración. Es claro que todo $g \in G$ puede expresarse de manera única en la forma $g = nu$, con $n \in N$ y $u \in U$. Definamos ahora

$$\psi : G \longrightarrow N \rtimes_\alpha U,$$

mediante $\psi(g) := (n, u)$. Se verifica que ψ está bien definida y es biyectiva. Demostramos ahora que ψ es un homomorfismo. Sean $g_1 = n_1u_1$, $g_2 = n_2u_2 \in G$. Entonces

$$\begin{aligned}g_1g_2 &= n_1u_1n_2u_2 \\ &= n_1u_1n_2(u_1^{-1}u_1)u_2 \\ &= n_1\alpha(u_1)(n_2)u_1u_2.\end{aligned}$$

En consecuencia,

$$\begin{aligned}\psi(g_1g_2) &= (n_1\alpha(u_1)(n_2), u_1u_2) \\ &= (n_1, u_1) \cdot (n_2, u_2) \\ &= \psi(g_1)\psi(g_2),\end{aligned}$$

con lo cual se tiene la afirmación. □

5.6 Ejercicios

1. `Demuestre o refute:`

(a) $\mathbb{Z}_8 \cong \mathbb{Z}_2 \times \mathbb{Z}_4$.

(b) $\mathbb{Z}_8 \cong \mathbb{Z}_2 \times V_4$.

2. `Demuestre o refute:` $\mathbb{Q}_8$ solo admite la descomposición trivial.

3. `Demuestre o refute:` Si el producto directo $G_1 \times H_1$ es isomorfo a $G_2 \times H_2$, entonces G_1 es isomorfo a G_2 y H_1 es isomorfo a H_2.

4. Demuestre el teorema 5.4.11.

5. Demuestre el teorema 5.2.6.

6. Demuestre el lema 5.2.7.

7. Sea $G = G_1 \times \cdots \times G_n$, $J = \{1, \ldots, n\}$ y sean I, K subconjuntos de J tales que $I \cap K = \varnothing$ y $I \cup K = J$. Entonces, G admite un subgrupo normal N isomorfo a $\prod_{i \in I} G_i$ y $G/N \cong \prod_{k \in K} G_k$.

8. Sean G y H grupos finitos con $\text{mcd}(|G|, |H|) = 1$. Demuestre que

$$\text{Aut}(G \times H) = \text{Aut}(G) \times \text{Aut}(H).$$

9. Sea G un grupo finito y $U, N \trianglelefteq G$ con $\text{mcd}(|U|, |N|) = 1$ y $|G| = |U|\,|N|$. Demuestre que

(a) $G = U \times N$.

(b) $\text{Aut}(G) \cong \text{Aut}(U) \times \text{Aut}(N)$.

10. Sea G y H grupos. Demuestre que $Z(G \times H) = Z(G) \times Z(H)$.

11. Sea G un grupo cíclico de orden p^n con p un número primo y $n \in \mathbb{N}$. Demuestre que $\text{Aut}(G) = S \times T$, donce $S, T \leq \text{Aut}(G)$, $|S| = p^{n-1}$ y T es un grupo cíclico de orden $p - 1$.

12. Determine todos los homomorfismos $\alpha : \mathbb{Z}_4 \longrightarrow \text{Aut}(\mathbb{Z}_5)$ y para cada uno de estos construya el producto semidirecto $\mathbb{Z}_5 \rtimes_\alpha \mathbb{Z}_4$. ¿Son estos grupos isomorfos?

13. Determine todos los homomorfismos $\alpha : \mathbb{Z}_2 \longrightarrow \text{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2)$ y para cada uno de estos construya el producto semidirecto $(\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_\alpha \mathbb{Z}_2$. ¿Son estos grupos isomorfos?

14. Sean $N_1, \ldots, N_k$ subgrupos normales de un grupo G. Demuestre que la función

$$\alpha : G \longrightarrow G/N_1 \times \cdots \times G/N_k$$

definida por

$$\alpha(g) = (gN_1, \ldots, gN_k)$$

es un homomofismo de grupos cuyo núcleo está dado por

$$\ker(\alpha) = \bigcap_{j=1}^{k} N_j.$$

En particular se cumple que $G/\bigcap_{j=1}^{k} N_j$ es isomorfo a un subgrupo de $G/N_1 \times \cdots \times G/N_k$.

15. Sea K un grupo y defina $\alpha : K \longrightarrow \mathrm{Sym}(K)$ mediante

$$\alpha(k) := \tau_k,$$

donde $\tau_k(x) = xk$ para todo $x \in K$.

(a) Demuestre que α es un homomorfismo de grupos.

(b) Sea H un grupo y defina $B := \prod_{k \in K} H_k$, donde cada $H_k \cong H$. Demuestre que $\mathrm{Sym}(K)$ puede verse como un subgrupo de $\mathrm{Aut}(B)$ de la siguiente manera: para todo $h_k \in H_k$, $k \in K$ y $\gamma \in \mathrm{Sym}(K)$ defina

$$\gamma(h_k) = h_{\gamma(k)}.$$

(c) Construya el producto demidirecto $G := H \rtimes_\alpha K$ y determine su orden. Este grupo G se denomina `producto orlado` de H con K. (En inglés *wreath product*).

(d) Demuestre que si H y K son grupos simples no abelianos, entonces B es el único subgrupo normal no trivial de G.

CAPÍTULO 6

LOS TEOREMAS DE SYLOW

Algunos conceptos y resultados introducidos y demostrados en el contexto de grupos *concretos* son ahora reformulados y reprobados en un contexto abstracto. Un ejemplo interesante de esto es la nueva demostración, en un contexto abstracto, de los teoremas de Sylow presentada en 1872 por F. Frobenius. Recordemos que Sylow demostró sus teoremas para grupos de permutaciones.
(A History of Abstract Algebra - Israel Kleiner)

A lo largo de este capítulo G denota siempre un grupo y Ω un conjunto no vacío.

Iniciamos este capítulo estudiando el concepto de **acción de un grupo sobre un conjunto**.

6.1 Representaciones por permutaciones y G-conjuntos

6.1.1 Definición. Un homomorfismo de grupos $\alpha : G \longrightarrow \mathrm{Sym}(\Omega)$ se denomina una **representación por permutaciones de** G sobre Ω. Esto es para todo $g \in G$ se verifica que $\alpha(g)$ es una permutación de Ω.

6.1.2 Definición. Decimos que G **actúa** a izquierda sobre Ω o que Ω es un G-**conjunto** izquierdo si a cada par $(g, \omega) \in G \times \Omega$ está asociado un elemento $g \cdot \omega \in \Omega$ tal que

(1) $1 \cdot \omega = \omega$ para todo $\omega \in \Omega$.

(2) $(gh) \cdot \omega = g \cdot (h \cdot \omega)$ para todo $g, h \in G$ y todo $\omega \in \Omega$.

6.1.3 Teorema. Las siguientes afirmaciones son equivalentes:

(1) Ω es un G-conjunto izquierdo.

(2) Existe una representación de G por permutaciones sobre Ω.

Demostración. (1) $\Rightarrow$ (2). Supongamos que está definida una acción $g \cdot \omega$ para todo $g \in G$ y $\omega \in \Omega$ y definamos $\alpha : G \longrightarrow \mathrm{Sym}(\Omega)$ mediante

$$\alpha(g)(\omega) = g \cdot \omega.$$

Demostramos que α es una representación por permutaciones de G sobre Ω.

(a) $\alpha(g)$ `es inyectiva para todo` $g \in G$. Sean $g \in G$ y $\omega_1, \omega_2 \in \Omega$. Entonces

$$\begin{aligned} \alpha(g)\omega_1 = \alpha(g)\omega_2 &\Leftrightarrow g \cdot \omega_1 = g \cdot \omega_2 \\ &\Rightarrow g^{-1} \cdot (g \cdot \omega_1) = g^{-1} \cdot (g \cdot \omega_2) \\ &\Rightarrow (gg^{-1}) \cdot \omega_1 = (gg^{-1}) \cdot \omega_2 \\ &\Rightarrow 1 \cdot \omega_1 = 1 \cdot \omega_2 \\ &\Rightarrow \omega_1 = \omega_2. \end{aligned}$$

(b) $\alpha(g)$ `es sobreyectiva para todo` $g \in G$. Sea $\omega \in \Omega$. Note que $g^{-1} \cdot \omega \in \Omega$ y se verifica que $\alpha(g)(g^{-1} \cdot \omega) = \omega$.

De (a) y (b) se sigue que $\alpha(g) \in \mathrm{Sym}(\Omega)$ para todo $g \in G$.

(c) α `es un homomorfismo.` Sean $g_1, g_2 \in G$ y $\omega \in \Omega$. Entonces

$$\begin{aligned} \alpha(g_1g_2)(\omega) &= (g_1g_2) \cdot \omega \\ &= g_1 \cdot (g_2 \cdot \omega) \\ &= \alpha(g_1)(\alpha(g_2)(\omega)) \\ &= (\alpha(g_1) \circ \alpha(g_2))(\omega). \end{aligned}$$

Por lo tanto, $\alpha(g_1g_2) = \alpha(g_1) \circ \alpha(g_2)$.

(2) $\Rightarrow$ (1). Recíprocamente, supongamos que $\alpha : G \longrightarrow \mathrm{Sym}(\Omega)$ es un homomorfismo de grupos y definamos una acción de G sobre Ω de la siguiente manera:

$$g \cdot \omega := \alpha(g)(\omega).$$

Verificamos que Ω es un G-conjunto.

(a) Sea $\omega \in \Omega$. Entonces $1 \cdot \omega = \alpha(1)(\omega) = \mathrm{I}_\Omega(\omega) = \omega$.

(b) Sean $\omega \in \Omega$ y $g, h \in G$. Entonces

$$\begin{aligned}(gh) \cdot \omega &= \alpha(gh)(\omega) \\ &= (\alpha(g) \circ \alpha(h))(\omega) \\ &= \alpha(g)(\alpha(h)(\omega)) \\ &= \alpha(g)(h \cdot \omega) \\ &= g \cdot (h \cdot \omega). \quad \square\end{aligned}$$

6.1.4 Ejemplos. (1) Sea $U \leq G$ y definamos $\Omega := \{U^x \mid x \in G\}$. Entonces

$$\alpha : G \longrightarrow \mathrm{Sym}(\Omega)$$

definida por

$$\alpha(g)(U^x) := U^{gx}$$

es una representación por permutaciones de G sobre Ω. Usando el teorema anterior se tiene que Ω es un G-conjunto mediante la acción definida por

$$g \cdot U^x := U^{gx}.$$

(2) Sea $U \leq G$ y $\Omega := \{gU \mid g \in G\}$ el conjunto de las clases laterales izquierdas de U en G. Entonces

$$\alpha : G \longrightarrow \mathrm{Sym}(\Omega)$$

definida por

$$\alpha(h)(gU) := hgU,$$

es una representación por permutaciones de G sobre Ω. Usando el teorema anterior se tiene que Ω es un G-conjunto mediante la acción definida por

$$h \cdot gU := hgU.$$

(3) Sea $\Omega = N \trianglelefteq G$. Entonces

$$\alpha : G \longrightarrow \mathrm{Sym}(\Omega)$$

definida por

$$\alpha(g)(n) := gng^{-1}$$

es una representación por permutaciones de G sobre Ω. Usando el teorema anterior se tiene que Ω es un G-conjunto mediante la acción definida por

$$g \cdot n := gng^{-1}.$$

6.1.5 Lema. Sea Ω un G-conjunto y sobre el conjunto Ω definamos la siguiente relación: dados $\omega_1, \omega_2 \in \Omega$

$$\omega_1 \sim \omega_2 \Leftrightarrow \exists g \in G \text{ tal que } \ g \cdot \omega_1 = \omega_2.$$

Entonces $\sim$ es una relación de equivalencia.

DEMOSTRACIÓN. (1) $\omega \sim \omega$, ya que $1\omega = \omega$ para todo $\omega \in \Omega$.

(2) Si $\omega_1 \sim \omega_2$, entonces existe $g \in G$ tal que $\omega_2 = g \cdot \omega_1$. En consecuencia, $g^{-1} \cdot \omega_2 = \omega_1$, es decir, $\omega_2 \sim \omega_1$.

(3) Si $\omega_1 \sim \omega_2$ y $\omega_2 \sim \omega_3$, entonces existen $g_1, g_2 \in g$ tales que $\omega_2 = g_1 \cdot \omega_1$ y $\omega_3 = g_2 \cdot \omega_2$. Por lo tanto, $\omega_3 = g_2 \cdot (g_1 \cdot \omega_1) = (g_2 g_1) \cdot \omega_1$, por lo que $\omega_1 \sim \omega_3$. □

6.1.6 Definición. (Órbita) Si $\omega \in \Omega$, entonces su clase de equivalencia bajo $\sim$ se denomina `órbita de` ω `bajo` G y se nota con $\mathrm{Orb}_G(\omega)$ o con ω^G. Es decir,

$$\mathrm{Orb}_G(\omega) = \{g \cdot \omega \mid g \in G\}.$$

6.1.7 Observación. Sea $T = \{\omega_j \mid j \in J\} \subseteq \Omega$ un sistema completo de representantes de $\sim$. Esto es,

(1) para todo $\omega \in \Omega$ existe $\omega_j \in T$ tal que $\omega \in \mathrm{Orb}_G(\omega_j)$ y

(2) para todo $\omega_1, \omega_2 \in T$ con $\omega_1 \neq \omega_2$ se tiene que $\mathrm{Orb}_G(\omega_1) \neq \mathrm{Orb}_G(\omega_2)$.

En este caso se verifica que $\{\mathrm{Orb}_G(\omega_j) \mid j \in J\}$ es una partición de Ω. Por lo tanto,

$$\Omega = \dot{\bigcup_{j \in J}} \mathrm{Orb}_G(\omega_j).$$

En particular, si Ω es finito, se tiene que $|\Omega| = \sum_{j \in J} |\mathrm{Orb}_G(\omega_j)|$.

6.1.8 Definición. (Estabilizador) Sea Ω un G-conjunto. Si $\omega \in \Omega$, entonces llamamos al conjunto

$$G_\omega := \{g \in G \mid g \cdot \omega = \omega\}$$

el `estabilizador` de ω en G.

6.1.9 Lema. Si Ω es un G-conjunto, entonces $G_\omega \leq G$ para todo $\omega \in \Omega$.

DEMOSTRACIÓN. Es claro que $1 \in G_\omega$, por lo tanto G_ω es no vacío. Sean $g, h \in G_\omega$ y $\omega \in \Omega$. Entonces $(gh^{-1}) \cdot \omega = g \cdot (h^{-1} \cdot \omega) = g \cdot \omega = \omega$. Esto demuestra que $G_\omega \leq G$. □

6.1.10 Teorema. (El estabilizador y la órbita) Sea Ω un G-conjunto. Entonces

$$|G : G_\omega| = |\mathrm{Orb}_G(\omega)|$$

para todo $\omega \in \Omega$.

Demostración. Note que

$$\begin{aligned} g \cdot \omega = h \cdot \omega &\Leftrightarrow h^{-1} \cdot (g \cdot \omega) = h^{-1} \cdot (h \cdot \omega) \\ &\Leftrightarrow (h^{-1}g) \cdot \omega = \omega \\ &\Leftrightarrow h^{-1}g \in G_\omega \\ &\Leftrightarrow g \in hG_\omega \\ &\Leftrightarrow gG_\omega = hG_\omega. \end{aligned}$$

En conclusión, G_ω tiene tantas clases laterales izquierdas distintas en G como elementos distintos tenga el conjunto $\mathrm{Orb}_G(\omega)$. □

6.1.11 Definición. Decimos que G opera `transitivamente` sobre un G-conjunto Ω o que Ω es un G-`conjunto transitivo` si para todo $\omega_1, \omega_2 \in \Omega$ existe $g \in G$ tal que $g \cdot \omega_1 = \omega_2$. Es decir, Ω es la única órbita de G sobre Ω.

6.1.12 Ejemplos. Consideremos nuevamente las acciones presentadas en el ejemplo 6.1.4.

(1) Sean $U \leq G$ y $\Omega := \{U^x \mid x \in G\}$. Consideremos la acción de G sobre Ω dada por $g \cdot U^x = U^{gx}$. Entonces Ω es la única órbita determinada por esta acción de G. Por lo tanto, Ω es un G-conjunto transitivo. Además

$$\begin{aligned} G_{U^x} &= \{g \in G \mid g \cdot U^x = U^x\} \\ &= \{g \in G \mid U^{gx} = U^x\} \\ &= \{g \in G \mid (U^x)^g = U^x\} \\ &= N_G(U^x). \end{aligned}$$

Dado que la acción es transitiva, del teorema del estabilizador y la órbita se sigue que

$$|\Omega| = |\{U^g \mid g \in G\}| = |G : N_G(U)|.$$

(2) Sea $U \leq G$ y $\Omega := \{gU \mid g \in G\}$ el conjunto de las clases laterales izquierdas de U en G. Se verifica que Ω es la única órbita determinada por la acción $h \cdot gU := hgU$. Además

$$\begin{aligned} G_{hU} &= \{g \in G \mid g \cdot hU = hU\} \\ &= \{g \in G \mid ghU = hU\} \\ &= \{g \in G \mid h^{-1}ghU = U\} \\ &= \{g \in G \mid h^{-1}gh \in U\} \\ &= \{g \in G \mid g \in hUh^{-1}\} \\ &= U^{h^{-1}}. \end{aligned}$$

(3) Sea $\Omega = N \trianglelefteq G$ y consideremos la acción de G sobre N por conjugación. La órbita de $n \in N$ está dada por

$$\mathrm{Orb}_G(n) = \{gng^{-1} \mid g \in G\}.$$

Esta se denomina `clase de conjugación` de n bajo G y se nota con $\mathrm{Cl}_G(n)$. Note además que

$$\begin{aligned} G_n &= \{g \in G \mid g \cdot n = n\} \\ &= \{g \in G \mid gng^{-1} = n\} \\ &= \{g \in G \mid gn = ng\} \\ &=: C_G(n). \end{aligned}$$

El conjunto $C_G(n)$ se denomina el `centralizador` de n en G.

6.1.13 Teorema. Sea Ω un G-conjunto. Entonces

(1) Si $T \subseteq \Omega$ es un sistema completo de representantes para las órbitas, entonces

$$|\Omega| = \sum_{\omega \in T} |G : G_\omega|. \tag{6.1}$$

(2) Si Ω es un G-conjunto transitivo finito, entonces $|G : G_\omega| = |\Omega|$ para todo $\omega \in \Omega$.

(3) Para todo $g \in G$ y todo $\omega \in \Omega$ se verifica que $G_{g\cdot\omega} = gG_\omega g^{-1}$.

Demostración. (1) Dado que Ω es la unión disyunta $\Omega = \bigcup_{\omega \in T} \mathrm{Orb}_G(\omega)$, usando el teorema del estabilizador y la órbita se tiene que

$$|\Omega| = \sum_{\omega \in T} |\mathrm{Orb}_G(\omega)| = \sum_{\omega \in T} |G : G_\omega|.$$

(2) Se sigue de (1).

(3) Sean $g \in G$ y $\omega \in \Omega$. Entonces

$$\begin{aligned} h \in G_{g\cdot\omega} &\Leftrightarrow h\cdot(g\cdot\omega) = g\cdot\omega \\ &\Leftrightarrow (hg)\cdot\omega = g\cdot\omega \\ &\Leftrightarrow (g^{-1}hg)\cdot\omega = \omega \\ &\Leftrightarrow g^{-1}hg \in G_\omega \\ &\Leftrightarrow h \in gG_\omega g^{-1}. \end{aligned}$$

6.1.14 Corolario. Sea G finito, Ω un G-conjunto finito y $n \in \mathbb{N}$. Entonces

(1) Si $n \mid |\mathrm{Orb}_G(\omega)|$ para todo $\omega \in \Omega$, entonces $n \mid |\Omega|$.

(2) La longitud de cualquier órbita, es decir, su número de elementos, divide a $|G|$. En particular, si G actúa transitivamente sobre Ω, entonces $|\Omega|$ divide a $|G|$.

Demostración. (1) Dado que Ω es la unión disjunta de las órbitas de G sobre Ω, el resultado se sigue del teorema anterior.

(2) Como consecuencia del teorema de Lagrange y del teorema anterior se tiene que

$$|G| = |G : G_\omega|\ |G_\omega| = |\mathrm{Orb}_G(\omega)|\ |G_\omega|,$$

con lo cual se tiene el resultado. □

6.1.15 Observación. Sea $\alpha : G \longrightarrow \mathrm{Sym}(\Omega)$ una representación por permutaciones de G sobre Ω. Entonces

$$\begin{aligned} \ker(\alpha) &= \{g \in G \mid \alpha(g) = I_\Omega\} \\ &= \{g \in G \mid g\cdot\omega = \omega,\ \forall\omega \in \Omega\} \\ &= \bigcap_{\omega\in\Omega} G_w. \end{aligned}$$

6.1.16 Ejemplos. (1) Si $U \leq G$ y $\Omega := \{U^x \mid x \in G\}$. Entonces para la acción de G sobre Ω dada por $g\cdot U^x := U^{gx}$ se tiene que

$$\ker(\alpha) = \bigcap_{x\in G} G_{U^x} = \bigcap_{x\in G} N_G(U^x).$$

(2) Sean $U \leq G$ y $\Omega := \{gU \mid g \in G\}$ y la acción de G sobre Ω dada por $h\cdot gU := hgU$. En este caso

$$\ker(\alpha) = \bigcap_{g\in G} G_{gU} = \bigcap_{g\in G} U^{g^{-1}} = \bigcap_{x\in G} U^x.$$

Este subgrupo normal de G se denomina el `core` de U en G y se nota con $\mathrm{Core}_G(U)$.

(3) Sean $\Omega = N \trianglelefteq G$ y consideremos la acción de G sobre N por conjugación. En este caso tenemos que

$$\ker(\alpha) = \bigcap_{n \in N} G_n = \bigcap_{n \in N} C_G(n) = Z(N).$$

6.1.17 Teorema. (Propiedades del Core) Sea $U \leq G$. Entonces

(1) $\mathrm{Core}_G(U) \trianglelefteq G$.

(2) $\mathrm{Core}_G(U) \leq U$.

(3) Si $M \trianglelefteq G$ y $M \leq U$, entonces $M \leq \mathrm{Core}_G(U)$. En consecuencia, $\mathrm{Core}_G(U)$ es el subgrupo más grande de G, que es normal en G y está contenido en U.

Demostración. (1) Dado que $\mathrm{Core}_G(U)$ es por definición el núcleo de un homomorfismo, se tiene la normalidad.

(2) Note que U es uno de los miembros de la intersección $\bigcap_{g \in G} U^g = \mathrm{Core}_G(U)$, por lo tanto, $\mathrm{Core}_G(U) \subseteq U$.

(3) Dado que $M \trianglelefteq G$ para todo $g \in G$ se verifica que $M^g = M$. Por otro lado, por hipótesis $M \leq U$, por consiguiente $M = M^g \leq U^g$ para todo $g \in G$. Esto demuestra que $M \leq \bigcap_{g \in G} U^g = \mathrm{Core}_G(U)$. □

6.1.18 Teorema. (Cayley) Sea $U \leq G$. Entonces $G/\mathrm{Core}_G(U)$ es isomorfo a un subgrupo de $\mathrm{Sym}(|G : U|)$. En particular, si $U = 1$, entonces G es isomorfo a un subgrupo de $\mathrm{Sym}(|G|)$.

Demostración. Si G es finito, entonces $|\Omega| = |G : U|$. Usando el primer teorema de isomorfía podemos afirmar que

$$\begin{aligned} G/\mathrm{Core}_G(U) &= G/\ker(\alpha) \\ &\cong \mathrm{Im}(\alpha) \\ &\leq \mathrm{Sym}(\Omega) \\ &\cong \mathrm{Sym}(|\Omega|). \end{aligned}$$

Es decir, $G/\mathrm{Core}_G(U)$ es isomorfo a un subgrupo de $\mathrm{Sym}(|G : U|)$. □

6.1.19 Definición. Sea Ω un G-conjunto. Decimos que $\omega \in \Omega$ es un `punto fijo` de la acción de G sobre Ω si $g \cdot \omega = \omega$ para todo $g \in G$.

6.1.20 Observación. Si ω es un punto fijo de la acción de G sobre Ω, entonces $\mathrm{Orb}_G(\omega) = \{\omega\}$ o, equivalentemente, $G_\omega = G$ y, en consecuencia, $|G : G_\omega| = 1$. Notamos con $\mathrm{Fix}_G(\Omega)$

el conjunto de todos los puntos fijos de la acción de G sobre Ω. Dado que $F \coloneqq \mathrm{Fix}_G(\Omega)$ está contenido en cualquier sistema de representantes T para las órbitas, la ecuación (6.1) en el teorema 6.1.13 se transforma en

$$|\Omega| = |\mathrm{Fix}_G(\Omega)| + \sum_{\omega \in T \setminus F} |G : G_\omega|. \tag{6.2}$$

6.1.21 Ejemplo. Si G es finito, entonces G actúa sobre sí mismo por conjugación. Si $x \in G$ es un punto fijo de esta acción, entonces $gxg^{-1} = x$ para todo $g \in G$. Es decir, $x \in Z(G)$. Por otro lado, recordemos que $G_x = C_G(x)$. Entonces en este caso con una reenumeración adecuada (6.2) se transforma en

$$|G| = |Z(G)| + \sum_{j=1}^{m} |G : C_G(h_j)|. \tag{6.3}$$

Esta igualdad es usualmente denominada `la ecuación de las clases` de G.

6.1.22 Lema. (Punto fijo) Sea $|G| = p^m$, donde p es un número primo y $m \in \mathbb{N}$. Sea Ω un G-conjunto finito con $p \nmid |\Omega|$. Entonces G tiene un punto fijo sobre Ω.

Demostración. Sea $T = \{\omega_1, \ldots, \omega_n\} \subseteq \Omega$ es un sistema de representantes para las órbitas. Entonces $\Omega = \bigcup_{j=1}^{n} \mathrm{Orb}_G(\omega_j)$ y se tiene que $|\mathrm{Orb}_G(\omega_j)| = |G : G_{\omega_j}| = p^{n_j}$, con $n_j \in \mathbb{N}_0$. Es decir,

$$|\Omega| = \sum_{j=1}^{n} p^{n_j}.$$

Si $n_j > 0$ para todo $j = 1, \ldots, n$, entonces $|\Omega| = pk$ para algún $k \in \mathbb{Z}$. Es decir, $p \mid |\Omega|$, lo cual contradice la hipótesis $p \nmid |\Omega|$. Entonces existe $j_0 \in \{1, \ldots, n\}$ tal que $|\mathrm{Orb}_G(\omega_{j_0})| = 1$. Es decir, ω_{j_0} es un punto fijo. □

6.1.23 Teorema. (Argumento de Frattini[1] I) Sean $N \trianglelefteq G$ y Ω un G-conjunto. Si Ω es un N-conjunto transitivo, entonces $G = G_\omega N$ para todo $\omega \in \Omega$.

Demostración. Es claro que para todo $\omega \in \Omega$ se verifica que $NG_\omega = G_\omega N \subseteq G$.

Sean $g \in G$ y $\omega \in \Omega$. Dado que Ω es un N-conjunto transitivo, existe $n \in N$ tal que $n \cdot \omega = g \cdot \omega$. Por lo tanto, $n^{-1}g \in G_\omega$. Es decir, $g \in nG_\omega$ y se tiene que $G \subseteq NG_\omega = G_\omega N$, con lo cual se tiene la afirmación. □

[1] Giovanni Frattini (1852-1925), matemático italiano. Conocido sobre todo por sus contribuciones a la teoría de grupos. No obstante, también se ocupó de la geometría diferencial y de la teoría de números de las formas cuadráticas binarias.

6.2 Los p-subgrupos de Sylow

A lo largo de esta sección todos los grupos considerados son finitos y p denota un número primo.

6.2.1 Definición. G se denomina p-`grupo` si $|G| = p^a$, con $a \in \mathbb{N}_0$.

6.2.2 Teorema. (Ferdinand Frobenius[2]) Sea $|G| = p^a m$ con $a \in \mathbb{N}$. Notemos con $N(p^a)$ al número de subgrupos de G con orden p^a. Entonces

$$N(p^a) \equiv 1 \bmod p.$$

En particular, G tiene por lo menos un subgrupo de orden p^a.

Demostración.(Helmut Wielandt[3], 1959) Sea Ω el conjunto definido por

$$\Omega := \{M \subseteq G \mid \ |M| = p^a\}.$$

Definamos sobre Ω la siguiente acción:

$$g \circ M := gM$$

para todo $g \in G$ y $M \in \Omega$. Entonces se verifica que Ω es un G-conjunto.

Sea $\Omega = \bigcup_j \Omega_j$ la descomposición de Ω en órbitas bajo G. Usando el teorema del estabilizador y la órbita, se sigue que

$$|\Omega_j| = |G : G_{M_j}|$$

para algún $M_j \in \Omega_j$. Entonces $G_{M_j} M_j = M_j$ y se tiene que

$$M_j = \bigcup_{k=1}^{n_j} G_{M_j} m_{jk}, \quad \text{con} \quad m_{jk} \in M_j.$$

En particular se cumple que

$$p^a = |M_j| = n_j |G_{M_j}|.$$

Es decir, $|G_{M_j}| = p^{b_j}$, con $b_j \leq a$. En consecuencia,

$$|\Omega_j| = |G : G_{M_j}| = \frac{|G|}{|G_{M_j}|} = \frac{p^a m}{p^{b_j}} = p^{a-b_j} m.$$

[2]Ferdinand Georg Frobenius (1849-1917), matemático alemán. Sus campos centrales de investigación fueron las ecuaciones diferenciales y la teoría de grupos.

[3]Helmut Wielandt (1910-2001), matemático alemán. Su principal campo de trabajo fue la teoría de grupos, especialmente la teoría de grupos de permutaciones. La prueba de Wielandt del teorema de Sylow es ahora estándar en todo el mundo.

Diferenciamos dos casos:

`Caso 1.` Si $b_j < a$, entonces $|\Omega_j| \equiv 0 \bmod (pm)$.

`Caso 2.` Si $b_j = a$, entonces $|\Omega_j| = m$ y tenemos

$$\begin{aligned} |\Omega| &= \sum_j |\Omega_j| \\ &= \sum_{|\Omega_j|=m} |\Omega_j| + \sum_{|\Omega_j|>m} |\Omega_j| \\ &= lm + \sum_{|\Omega_j|>m} |\Omega_j|, \end{aligned}$$

donde l es el número de órbitas con m elementos. Por lo tanto,

$$|\Omega| \equiv lm \bmod (pm). \tag{6.4}$$

Demostramos ahora que $N(p^a) = l$. Para ello consideremos los conjuntos

$$\begin{aligned} \mathfrak{M} &= \{V \mid V \leq G,\ |V| = p^a\}, \\ \mathfrak{N} &= \{\Omega_j \mid |\Omega_j| = m\} \end{aligned}$$

y definamos la función $\tau : \mathfrak{M} \longrightarrow \mathfrak{N}$ mediante

$$\tau(V) := \{g \circ V \mid g \in G\}.$$

(1) $\tau(V) \in \mathfrak{N}$. Si $V \in \mathfrak{M}$, entonces $\tau(V)$ es una órbita, y además

$$|\tau(V)| = |G : V| = \frac{p^a m}{p^a} = m.$$

(2) τ `es inyectiva.` Supongamos que $\tau(V_1) = \tau(V_2)$. Entonces existe $g \in G$ tal que $V_1 = gV_2$. En particular se cumple que $e = gh$ para algún $h \in V_2$. Es decir, $g \in V_2$ y se tiene que $V_1 = V_2$.

(3) τ `es sobre.` Sea $\Omega_j \in \mathfrak{N}$, $M \in \Omega_j$ y $U = G_M$, el estabilizador de M en G. Entonces $m = |\Omega_j| = |G : U|$ y se tiene que $|U| = p^a$.

Por otro lado, $M = \bigcup_{i=1}^{k} Um_i$, con $m_i \in M$. Es decir, $p^a = k|U| = kp^a$, con lo cual se sigue que $k = 1$ y $M = Um_1$.

Note que

$$\begin{aligned}\Omega_j &= \{gM \mid g \in G\}\\ &= \{gUm_1 \mid g \in G\}\\ &= \{gm_1^{-1}Um_1 \mid g \in G\}\\ &= \{gU^{m_1^{-1}} \mid g \in G\}\\ &= \tau(U^{m_1^{-1}}).\end{aligned}$$

Todo lo anterior nos permite concluir que $N(p^a) = l$.

Retomando la congruencia (6.4) tenemos

$$|\Omega| \equiv N(p^a)m \bmod (pm). \tag{6.5}$$

Esta congruencia se verifica para todo grupo con orden $p^a m$. Por lo tanto, también es válida para el grupo cíclico con este orden. Para este se tiene que $N(p^a) = 1$. Por consiguiente,

$$|\Omega| \equiv m \bmod (pm).$$

Usando (6.5) tenemos

$$N(p^a)m \equiv m \bmod (pm),$$

por lo tanto,

$$N(p^a) \equiv 1 \bmod p. \quad \square$$

6.2.3 Corolario. Si $|G| = p^a m$, entonces para cada $j = 1, \ldots, a$ existe un subgrupo de G con orden p^j.

Demostración. Se sigue inmediatamente del teorema anterior. Tenga en cuenta que en este no se exigió que $p \nmid m$. $\square$

6.2.4 Corolario. (Cauchy[4]) Si $p \mid |G|$, entonces existe $g \in G$ con $\operatorname{ord}(g) = p$.

Demostración. Del teorema anterior se sigue que G admite un subgrupo U con $|U| = p$. Entonces U es cíclico, generado por un elemento g de orden p. $\square$

6.2.5 Definición. Sea $|G| = p^a m$ con $p \nmid m$. Si $U \leq G$, con $|U| = p^a$, entonces decimos que U es un p-`subgrupo de Sylow` de G. El conjunto de todos los p-subgrupos de Sylow de G lo notamos con $\mathrm{Syl}_p(G)$.

[4]Augustin Louis Cauchy (1789-1857), matemático francés. Cauchy fue pionero en el análisis y la teoría de grupos. También trabajó en análisis, especialmente en la convergencia y la divergencia de las series infinitas, ecuaciones diferenciales, determinantes, probabilidad y física matemática.

6.2.6 Teorema. (Ludwig Sylow[5], 1872) Sea $|G| = p^a m$ con $p \nmid m$. Entonces

(1) $\mathrm{Syl}_p(G) \neq \varnothing$.

(2) Si U es un p-subgrupo de G y $P \in \mathrm{Syl}_p(G)$, entonces existe $g \in G$ tal que $U \leq P^g$. En particular, dos p-subgrupos de Sylow de G son conjugados. Es decir, Si $P_1, P_2 \in \mathrm{Syl}_p(G)$, entonces existe $g \in G$ tal que $P_1^g = P_2$.

(3) $|\mathrm{Syl}_p(G)| = |G : N_G(P)| \equiv 1 \bmod p$. Mas aún, $|\mathrm{Syl}_p(G)| \mid m$, y por lo tanto $|\mathrm{Syl}_p(G)| \mid |G|$.

Demostración. (1) Se sigue del teorema de Frobenius. Note que $N(p^a) \neq 0$.

(2) Sea $P \in \mathrm{Syl}_p(G)$. Definamos el conjunto $\Omega := \{P^g \mid g \in G\}$. Del ejemplo 6.1.4 (3) se sigue que Ω es un G-conjunto transitivo bajo la acción

$$h \circ P^g := P^{hg}.$$

Usando el teorema del estabilizador y la órbita se sigue que $|\Omega| = |G : N_G(P)|$. Dado que $P \leq N_G(P) \leq G$, se verifica que

$$\begin{aligned} p^a m &= |G| \\ &= |G : N_G(P)| \; |N_G(P) : P| \; |P| \\ &= |\Omega| \; n \; p^a. \end{aligned}$$

Es decir, $m = n|\Omega|$. Por lo tanto, $p \nmid |\Omega|$.

Se verifica también que bajo la misma acción Ω es un U-conjunto. Del teorema del punto fijo se sigue que existe $g \in G$ tal que

$$P^{ug} = P^g \quad \forall u \in U.$$

Esto demuestra que $U \leq N_G(P^g)$ y se tiene que $UP^g \leq G$. Por lo tanto,

$$|UP^g| = \frac{|U| \; |P^g|}{|U \cap P^g|} = \frac{p^b p^a}{p^c} \leq p^a.$$

Dado que $U \cap P^g \leq U$, se sigue que $p^c \mid p^b$. En consecuencia, $p^b = p^c$. Es decir, $|U \cap P^g| = |U|$ y se tiene que $U = U \cap P^g \leq P^g$.

[5]Peter Ludwig Mejdell Sylow (1832-1918). Matemático noruego. Estudió en la universidad de Cristianía. Sus campos de investigación fueron inicialmente las funciones elípticas y después la solubilidad de ecuaciones algebráicas por radicales. En su paso por Berlin intercambió opiniones con Kronecker.

Para demostrar la segunda afirmación, sean $P_1, P_2 \in \mathrm{Syl}_p(G)$. Entonces existen $g, h \in G$ tales que $P_1 \leq P_2^g$ y $P_2 \leq P_1^h$. Por lo tanto,

$$|P_1| \leq |P_2^g| = |P_2| \leq |P_1^h| = |P_1|.$$

En conclusión, $|P_1| = |P_2^g|$ y así $P_1 = P_2^g$.

(3) Nuevamente del teorema del estabilizador y la órbita se sigue que $|G : N_G(P)|$ coincide con el número de conjugados de P en G. Pero todos los p-subgrupos de Sylow de G son conjugados en G. Es decir,

$$|\mathrm{Syl}_p(G)| = |G : N_G(P)| \equiv 1 \bmod p.$$

Por otro lado, dado que $P \leq N_G(P)$, tenemos

$$\begin{aligned} |\mathrm{Syl}_p(G)| &= \frac{|G|}{|N_G(P)|} \\ &= \frac{|G|}{|N_G(P) : P||P|} \\ &= \frac{m}{|N_G(P) : P|}. \end{aligned}$$

Es decir, se verifica que $|\mathrm{Syl}_p(G)| \mid m$. □

6.2.7 Observaciones. (1) Si $p \nmid |G|$, entonces $\mathrm{Syl}_p(G) = \{1\}$.

(2) Si $|G| = p^a$, entonces $\mathrm{Syl}_p(G) = \{G\}$.

6.2.8 Corolario. Sea $P \in \mathrm{Syl}_p(G)$. Entonces $P \trianglelefteq G$ si y solo si $\mathrm{Syl}_p(G) = \{P\}$. En este caso P consta de todos los elementos de G cuyos órdenes son p-potencias.

Demostración. Es consecuencia inmediata de los teoremas de Sylow. □

6.2.9 Ejemplos. Subgrupos de Sylow:

(1) $\mathrm{Syl}_2(\mathrm{Sym}(3)) = \{\langle(12)\rangle, \langle(13)\rangle, \langle(23)\rangle\}$.

(2) $\mathrm{Syl}_3(\mathrm{Sym}(3)) = \{\langle(123)\rangle\}$.

(3) $\mathrm{Syl}_3(\mathrm{Alt}(4)) = \{\langle(123)\rangle, \langle(124)\rangle, \langle(243)\rangle, \langle(134)\rangle\}$.

(4) $\mathrm{Syl}_2(\mathrm{Sym}(4)) = \{\langle(1234), (24)\rangle, \langle(1243), (23)\rangle, \langle(1324), (34)\rangle\}$.

6.2.10 Teorema. Si todos los subgrupos de Sylow de G (*i.e.* para cualquier número primo) son normales en G, entonces G es el producto directo de estos.

Demostración. Sea $|G| = p_1^{a_1} \cdots p_k^{a_k}$, con $p_i \neq p_j$ para cada $i \neq j$ la descomposición en factores primos de $|G|$. Por hipótesis, para cada $j \in \{1, \ldots, k\}$ existe un único p_j-subgrupo de Sylow de G, digamos P_j.

Si definimos $H := P_1 \cdots P_k$, entonces se tiene que $H \leq G$. Del toerema de Lagrange se sigue que $p_j^{a_j} \mid |H|$ para todo $j \in \{1, \ldots, k\}$. Dado que para cada $i \neq j$ se verifica que $\mathrm{mcd}(p_i, p_j) = 1$, tenemos que

$$p_1^{a_1} \cdots p_k^{a_k} \mid |H|.$$

Entonces $|G| \mid |H|$ y se sigue que $G = H$.

Sean ahora $g \in P_i$, $h \in P_j$, con $i \neq j$. Entonces

$$P_j \ni (ghg^{-1})h^{-1} = g(hg^{-1}h^{-1}) \in P_i.$$

En consecuencia, dado que $P_i \cap P_j = 1$, se tiene que $ghg^{-1}h^{-1} = 1$. Es decir, $gh = hg$. La conclusión se sigue del teorema 5.2.3. □

6.2.11 Corolario. Sea $|G| = p^a m$, con $p \nmid m$. Entonces

(1) $P \in \mathrm{Syl}_p(G)$ si y solo si P es un p-subgrupo maximal de G.

(2) Si $P \in \mathrm{Syl}_p(G)$ y $\alpha \in \mathrm{Aut}(G)$, entonces $\alpha(P) \in \mathrm{Syl}_p(G)$.

Demostración. (1) Sean $P \in \mathrm{Syl}_p(G)$ y U un p-subgrupo de G con $P \leq U < G$. Entonces $|U| \leq p^a = |P|$. Por lo tanto, $P = U$.

Recíprocamente, si P es un p-subgrupo maximal de G, entonces del segundo teorema de Sylow se sigue que $P \leq P_1$ para algún $P_1 \in \mathrm{Syl}_p(G)$. Por lo tanto, $P = P_1$.

(2) Dado que $\alpha \in \mathrm{Aut}(G)$, se sigue que $|\alpha(P)| = |P|$. Por lo tanto, $\alpha(P) = P_1^g$ para algún $P_1 \in \mathrm{Syl}_p(G)$ y algún $g \in G$. □

6.2.12 Lema. (Argumento de Frattini II.) Sea $|G| = p^a m$, con $p \nmid m$. Si $N \trianglelefteq G$ y $P \in \mathrm{Syl}_p(N)$, entonces $G = N_G(P)N$.

Demostración. Definamos $\Omega := \mathrm{Syl}_p(N)$. Es decir,

$$\Omega = \{P^n \mid n \in N\}.$$

Similar como antes, se verifica que Ω es un G-conjunto y además un N-conjunto transitivo. Usando el Argumento de Frattini I (teorema 6.1.23) se sigue que $G = N_G(P)N$. Tenga en cuenta que $N_G(P)$ coincide con el estabilizador de P en G. □

6.2.13 Corolario. Sea $|G| = p^a m$, con $p \nmid m$. Entonces

(1) Si $P \in \mathrm{Syl}_p(G)$ y $N_G(P) \leq U \leq G$, entonces $N_G(U) = U$.

(2) Si $P \in \mathrm{Syl}_p(G)$, entonces $N_G(N_G(P)) = N_G(P)$.

Demostración. (1) Es claro que $U \trianglelefteq N_G(U)$. Dado que $P \leq N_G(P) \leq U$, se sigue que $P \in \mathrm{Syl}_p(U)$. Usando el Argumento de Frattini II se tiene

$$N_G(U) = U \underbrace{N_{N_G(U)}(P)}_{\leq N_G(P) \leq U} = U.$$

(2) Se sigue de (1). □

6.2.14 Lema. Sean $U, V, W \leq G$. Entonces son equivalentes:

(1) $U \cap VW = (U \cap V)(U \cap W)$.

(2) $UV \cap UW = U(V \cap W)$.

Demostración. (1) $\Rightarrow$ (2). Dado que $V \cap W \subseteq V$ y $V \cap W \subseteq W$, se sigue que $U(V \cap W) \subseteq UV$ y $U(V \cap W) \subseteq UW$. Por lo tanto, $U(V \cap W) \subseteq (UV \cap UW)$. Sea ahora $z \in (UV \cap UW)$. Entonces existen $u, u' \in U$, $v \in V$ y $w \in W$ tales que $z = uv = u'w$. Por lo tanto, que $u^{-1}u' = vw^{-1} \in U \cap VW = (U \cap V)(U \cap W)$.

Entonces $vw^{-1} = v_1 w_1$, con $v_1 \in (U \cap V)$ y $w_1 \in (U \cap W)$. En consecuencia, $v_1^{-1} v = w_1 w \in (V \cap W)$. Entonces $z = uv = (uv_1)(v_1^{-1} v) \in U(V \cap W)$ y se tiene que $UV \cap UW \subseteq U(V \cap W)$. Esto demuestra que $(UV \cap UW) \subseteq U(V \cap W)$ y se tiene la igualdad.

(2) $\Rightarrow$ (1). Evidentemente, $(U \cap V)(U \cap W) \subseteq U \cap VW$. Sea ahora $z \in (U \cap VW)$. Entonces existen $u \in U$, $v \in V$ y $w \in W$ tales que $z = u = vw$. En consecuencia, $v = uw^{-1} \in (UV \cap UW) = U(V \cap W)$. Entonces $v = uw^{-1} = u_1 v_1$, con $u_1 \in U$ y $v_1 \in V \cap W$. Se sigue, por lo tanto, que $v_1 w = u_1^{-1} u$ y $u_1 = v v_1^{-1} \in (U \cap V)$. Entonces $z = u = vw = u_1(v_1 w) \in (U \cap V)(U \cap W)$. Esto demuestra que $U \cap VW \subseteq (U \cap V)(U \cap W)$. □

6.2.15 Teorema. Sea $|G| = p^a m$, con $p \nmid m$. Entonces

(1) Si $P \in \mathrm{Syl}_p(G)$ y $N \trianglelefteq G$, entonces $P \cap N \in \mathrm{Syl}_p(N)$ y $PN/N \in \mathrm{Syl}_p(G/N)$.

(2) Si $P \in \mathrm{Syl}_p(G)$ y $N_1, N_2 \trianglelefteq G$, entonces $N_1 N_2 \cap P = (N_1 \cap P)(N_2 \cap P)$ y $PN_1 \cap PN_2 = P(N_1 \cap N_2)$.

(3) Sea $|G| = p_1^{a_1} \cdots p_n^{a_n}$, con cada p_j un número primo y $p_i \neq p_j$, para $i \neq j$. Si $P_j \in \mathrm{Syl}_{p_j}(G)$, entonces $G = \langle P_j \mid j = 1, \ldots, n \rangle$. En particular, si $n = 2$, entonces $G = P_1 P_2$.

Demostración. (1) Dado que $N \trianglelefteq G$, se verifica que $PN \leq G$. Entonces

$$|N : P \cap N| = \frac{|N|}{|P \cap N|} = \frac{|P||N|}{|P||P \cap N|} = \frac{|PN|}{|P|} = |PN : P|. \tag{6.6}$$

y

$$|G/N : PN/N| = \frac{|G/N|}{|PN/N|} = \frac{|G|}{|PN|} = |G : PN|. \tag{6.7}$$

Por otro lado, dado que $|G : P| = |G : PN||PN : P|$ y dado que $p \nmid |G : P|$, se verifica que $p \nmid |PN : P|$ y $p \nmid |G : PN|$. Entonces

(a) $p \nmid |N : N \cap P|$. Por lo tanto, $P \cap N \in \mathrm{Syl}_p(N)$.

(b) $p \nmid |G : PN|$. En consecuencia, $PN/N \in \mathrm{Syl}_p(G/N)$.

(2) Es claro que $(N_1 \cap P)(N_2 \cap P) \leq N_1 N_2 \cap P$.

Si $M \leq G$, denotemos con $|M|_p$ la mayor potencia de p que divide a $|M|$. Es decir, si $|M| = p^b k$, con $p \nmid k$, entonces $|M|_p = p^b$.

De (1) se sigue que $|N_j \cap P| = |N_j|_p$ para $j = 1, 2$. Así, $|N_1 N_2 \cap P| = |N_1 N_2|_p$. Entonces

$$\begin{aligned} |(N_1 \cap P)(N_2 \cap P)| &= \frac{|N_1 \cap P||N_2 \cap P|}{|N_1 \cap N_2 \cap P|} \\ &= \frac{|N_1|_p |N_2|_p}{|N_1 \cap N_2|_p} \\ &= |N_1 N_2|_p \\ &= |N_1 N_2 \cap P|, \end{aligned}$$

con lo cual se tiene la igualdad. La otra afirmación se sigue del lema anterior.

(3) Definamos $U := \langle P_j \mid j = 1, \ldots, n \rangle \leq G$. Del teorema de Lagrange se sigue que

$$|P_j| \mid |U|, \quad \forall j = 1, \ldots, n.$$

Teniendo en cuenta que $\mathrm{mcd}(p_1^{a_1}, \ldots, p_n^{a_n}) = 1$, se demuestra por inducción que si $p_j^{a_j} \mid |U|$ para todo $j = 1, \ldots, n$, entonces $p_1^{a_1} \cdots p_n^{a_n} \mid |U|$. Por lo tanto, $|G| \mid |U|$ y se sigue que $U = G$.

Si $n = 2$, entonces $|P_1 P_2| = \frac{|P_1||P_2|}{|P_1 \cap P_2|} = |P_1||P_2| = |G|$. Por lo cual, $G = \langle P_1, P_2 \rangle = P_1 P_2$. □

6.3 Algunas aplicaciones

A lo largo de esta sección todos los grupos considerados son finitos y p y q denotan números primos.

6.3.1 Teorema. El grupo $\mathrm{Alt}(4)$ no tiene subgrupos de orden 6.

Demostración. Supongamos que $\mathrm{Alt}(4)$ admite un subgrupo U de orden 6. Dado que $|\mathrm{Alt}(4) : U| = 2$, se tiene que $U \lhd \mathrm{Alt}(4)$. Como consecuencia del tercer teorema de Sylow se sigue que

$$|\mathrm{Syl}_3(U)| \equiv 1 \bmod 3 \quad \text{y} \quad |\mathrm{Syl}_3(U)| \mid 2.$$

Es decir, $|\mathrm{Syl}_3(U)| \in \{1, 4, 7, \ldots\}$ y $|\mathrm{Syl}_3(U)| \mid 2$. Por consiguiente, $|\mathrm{Syl}_3(U)| = 1$, y así existe un único 3-subgrupo de Sylow de U, digamos P.

Para todo $g \in \mathrm{Alt}(4)$ se verifica que $P^g \subseteq U^g = U$. En consecuencia, $P^g = P$ y se sigue que $P \trianglelefteq \mathrm{Alt}(4)$. Pero $P \in \mathrm{Syl}_3(\mathrm{Alt}(4))$ y se sigue que $\mathrm{Alt}(4)$ tendría un único 3-subgrupo de Sylow, una contradicción. Ver ejemplo 6.2.9 (3). □

6.3.2 Teorema. Si $|G| = 20$, entonces G no es simple.

Demostración. Dado que $20 = 2^2 \cdot 5$, se verifica que $|\mathrm{Syl}_5(G)| \equiv 1 \bmod 5$ y también $|\mathrm{Syl}_5(G)| \mid 4$. Por lo cual, $|\mathrm{Syl}_5(G)| = 1$ y se tiene que existe un único 5-subgrupo de Sylow de G, por lo tanto, normal.

6.3.3 Teorema. Si $|G| = pq$, donde $2 \leq p < q$. Entonces

(1) G admite un único subgrupo de orden q, el cual es cíclico y además normal.

(2) Si $q \not\equiv 1 \bmod p$, entonces G admite un único subgrupo de orden p, el cual es cíclico y normal en G.

(3) Si $q \equiv 1 \bmod p$, entonces G admite un único subgrupo de orden p, el cual es cíclico y normal en G o bien admite q subgrupos de orden p, cíclicos y conjugados entre sí.

(4) G es el producto semidirecto de un q-subgrupo normal N y un p-subgrupo U.

(5) Si G admite un único subgrupo U de orden p, entonces $G \cong \mathbb{Z}_{pq}$.

Demostración. De los teoremas de Sylow se sigue que

$$|\mathrm{Syl}_q(G)| \equiv 1 \bmod q \quad \text{y} \quad |\mathrm{Syl}_q(G)| \mid p \tag{6.8}$$

y

$$|\mathrm{Syl}_p(G)| \equiv 1 \bmod p \quad \text{y} \quad |\mathrm{Syl}_p(G)| \mid q. \tag{6.9}$$

(1) De la segunda condición en (6.8) se sigue que $|\mathrm{Syl}_q(G)| \in \{1, p\}$. Dado que $p < q$, no puede verificarse la condición $|\mathrm{Syl}_q(G)| \equiv 1 \bmod q$. Por lo cual, $|\mathrm{Syl}_q(G)| = 1$. Entonces el único q-subgrupo de Sylow de G es normal y además cíclico por tener orden un número primo.

(2) De la última condición en (6.9) se sigue que $|\mathrm{Syl}_p(G)| \in \{1, q\}$. Dado que debe cumplirse que $\mathrm{Syl}_p(G)| \equiv 1 \bmod p$ y por hipótesis $q \not\equiv 1 \bmod p$, se tiene que $|\mathrm{Syl}_p(G)| = 1$. Entonces el único p-subgrupo de Sylow de G es normal y además cíclico por tener orden un número primo.

(3) Si $q \equiv 1 \bmod p$, entonces con el análisis anterior podemos afirmar que pueden darse las opciones $|\mathrm{Syl}_p(G)| = 1$ o $|\mathrm{Syl}_p(G)| = q$, con lo cual se tiene la afirmación.

(4) La existencia de tales subgrupos N y U está garantizada por lo anterior y del teroema 6.2.15 (3) se sigue que $G = UN$.

(5) En este caso, además de las condiciones $N \trianglelefteq G$, $G = UN$ y $U \cap N = 1$ se tiene que $U \trianglelefteq G$. Entonces

$$G = U \times N \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}.$$

Esta última isomorfía se sigue del hecho que $\mathrm{mcd}(p, q) = 1$. □

6.3.4 Corolario. Sea G un grupo con $|G| = 2p$ y p un número primo impar. Entonces $G \cong \mathbb{Z}_{2p}$ o $G \cong D_{2p}$.

Demostración. Del teorema 6.3.3 (1) se sigue que G admite un único subgrupo normal cíclcio de orden p, digamos $\langle a \rangle$, con $a \in G$. Del teorema de Cauchy se sigue que existe $b \in G$, con $\mathrm{ord}(b) = 2$. Dado que $\langle a \rangle \trianglelefteq G$, se sigue que

$$bab^{-1} = bab \in \langle a \rangle.$$

Es decir, $bab = a^j$ para algún $j \in \{1, \ldots, p-1\}$.

Si $r \in \mathbb{N}$, entonces, dado que b es una involución, se tiene que

$$ba^r b = (bab)^r = (a^j)^r = a^{rj}.$$

Entonces

$$a = b^2 ab^2 = b(bab)b = ba^j b = a^{j^2}$$

y, en consecuencia,

$$a^{j^2-1} = 1.$$

Dado que $\mathrm{ord}(a) = p$, se sigue que $p \mid j^2 - 1$ o, equivalentemente, $j^2 \equiv 1 \bmod p$. Las soluciones a esta congruencia son $j = 1$ o $j = p - 1$.

- Si $j = 1$, entonces $ab = ba$ y se tiene que G es abeliano, por lo tanto, isomorfo a $\mathbb{Z}_{2p}$.
- Si $j = p - 1$, entonces

$$G \cong \langle a, b \mid a^p = b^2 = 1,\ bab^{-1} = a^{p-1} \rangle \cong D_{2p},$$

con lo cual se concluye la prueba. □

6.3.5 Corolario. Existen salvo isomorfía dos grupos de orden 6.

Demostración. Del teorema anterior se sigue que existen, salvo isomorfía, los grupos $\mathbb{Z}_6$ y D_3. Usando el ejemplo 1.2.18 (simetrías del triángulo) se tiene que $D_3 \cong \mathrm{Sym}(3)$. □

6.3.6 Teorema. (Fórmula de conteo) Si G es un grupo finito, entonces

(1) $\bigcup_{P \in \mathrm{Syl}_p(G)} P = \{1\} \cup \{g \in G \mid \mathrm{ord}(g) = p^j, \text{con } j \geq 1\}$.

(2) Si la intersección de cualquier par de p-subgrupos de Sylow de G es trivial, entonces

$$|\{g \in G \mid \mathrm{ord}(g) = p^j, \text{con } j \geq 1\}| = |\mathrm{Syl}_p(G)|(|P| - 1),$$

donde $P \in \mathrm{Syl}_p(G)$.

Demostración. (1) Sea $g \in G$ con $\mathrm{ord}(g) = p^j$, $j \geq 1$. Entonces $\langle g \rangle$ es un p-subgrupo de G, el cual está contenido en un p-subgrupo de Sylow P de G. Esto demuestra que

$$\bigcup_{P \in \mathrm{Syl}_p(G)} P \supseteq \{1\} \cup \{g \in G \mid \mathrm{ord}(g) = p^j, \text{con } j \geq 1\}.$$

La otra inclusión es evidente.

(2) Note que

$$\begin{aligned} |\{g \in G \mid \mathrm{ord}(g) = p^j, \text{con } j \geq 1\}| &= \left| \bigcup_{P \in \mathrm{Syl}_p(G)}^{\cdot} (P \setminus \{1\}) \right| \\ &= \sum_{P \in \mathrm{Syl}_p(G)} |P \setminus \{1\}| \\ &= |\mathrm{Syl}_p(G)|(|P| - 1). \end{aligned}$$

6.3.7 Ejemplo. Sea $|G| = 12 = 2^2 3$. Demostramos que $|\mathrm{Syl}_2(G)| = 1$ o $|\mathrm{Syl}_3(G)| = 1$. Supongamos que $|\mathrm{Syl}_3(G)| \neq 1$. Entonces $|\mathrm{Syl}_3(G)| = 4$, ya que $|\mathrm{Syl}_3(G)| \equiv 1 \bmod 3$. Dado que los 3-subgrupos de Sylow de G son cíclicos de orden 3, aplicando la fórmula de conteo se tiene que G admite $4(3-1) = 8$ elementos de orden 3. En consecuencia, restan $12 - 8 = 4$ elementos, que deben formar un 2-subgrupo de Sylow. Es decir, $|\mathrm{Syl}_2(G)| = 1$.

6.4 Grupos abelianos finitos y finitamente generados

Similar como se realizo con los grupos cíclicos, la tarea principal de esta capítulo es clasificar los grupos abelianos finitos.

6.4.1 Lema. Sea $1 \neq G$ un p-grupo abeliano finito. Entonces G es cíclico si y solo si G tiene un único subgrupo de orden p.

Demostración. Si G es cíclico, entonces el resultado se sigue del teorema 4.2.3.

Recíprocamente, supongamos que $|G| = p^m$ y demostramos la afirmación por inducción sobre m. Si $m = 1$, entonces G es cíclico.

Supongamos entonces que $m > 1$ y que G admite un único subgrupo de orden p, digamos P. Entonces la función $\varepsilon : G \longrightarrow G$ definida por $\varepsilon(x) := x^p$ es un endomorfismo con

$$\ker(\varepsilon) = \{x \in G \mid x^p = 1\} = P.$$

Entonces del primer teorema de isomorfía se sigue que $G/P \cong \mathrm{Im}(\varepsilon)$. En consecuencia, $|\mathrm{Im}(\varepsilon)| = p^{m-1}$. Usando el teorema de Cauchy y la hipótesis se sigue que P es el único subgrupo de orden p de $\mathrm{Im}(\varepsilon) \leq G$.

Usando la hipótesis inductiva se sigue que $\mathrm{Im}(\varepsilon)$ es cíclico, digamos $\mathrm{Im}(\varepsilon) = \langle \varepsilon(g) \rangle$ para algún $g \in G$. Entonces $\mathrm{ord}(\varepsilon(g)) = \mathrm{ord}(g^p) = p^{m-1}$. Por lo tanto, $\mathrm{ord}(g) = p^m$ y se tiene que $G = \langle g \rangle$. □

6.4.2 Lema. Sea $1 \neq G$ un p-grupo abeliano finito y $g \in G$ con orden maximal. Entonces existe $U \leq G$ tal que $G = \langle g \rangle \times U$. Es decir, $\langle g \rangle$ tiene un `complemento` en G.

Demostración. Demostramos la afirmación por inducción sobre $|G|$. Si G es cíclico, entonces $G = \langle g \rangle$ para algún $g \in G$ con orden maximal y podemos tomar $U := 1$.

Supongamos entonces que G no es cíclico. Usando el lema anterior podemos afirmar que G tiene por lo menos dos subgrupos de orden p. Dado que $\langle g \rangle$ admite un único subgrupo de orden p, se tiene que existe $A \leq G$, con $|A| = p$, $A \not\leq \langle g \rangle$ y $A \cap \langle g \rangle = 1$.

Definamos $\overline{G} := G/A$ y $\overline{g} := gA \in \overline{G}$. Entonces usando el segundo teorema de isomorfía tenemos:

$$\langle \overline{g} \rangle = \langle g \rangle A/A \cong \langle g \rangle / (\langle g \rangle \cap A) \cong \langle g \rangle.$$

Por lo tanto, $\mathrm{ord}(\overline{g}) = \mathrm{ord}(g)$ y se tiene que $\overline{g}$ es un elemento con orden maximal en $\overline{G}$.

Usando la hipótesis de inducción se tiene que $\langle \overline{g} \rangle$ tiene un complemento en $\overline{G}$. Es decir, existe $\overline{U} \leq \overline{G}$ tal que $\overline{G} = \langle \overline{g} \rangle \times \overline{U}$. Sea $\overline{U} = U/A$. Entonces se verifica que

$$G = \langle g \rangle U \quad \text{y} \quad \langle g \rangle \cap U \leq A.$$

Dado que $A \cap \langle g \rangle = 1$, se tiene que $U \cap \langle g \rangle = 1$. Esto demuestra que $G = \langle g \rangle \times U$. □

6.4.3 Teorema. Sea $1 \neq G$ un p-grupo abeliano finito. Entonces G es un producto directo de grupos cíclicos. Si

$$G = \langle g_1 \rangle \times \cdots \times \langle g_n \rangle = \langle h_1 \rangle \times \cdots \times \langle h_m \rangle,$$

entonces $m = n$, y para una enumeración adecuada se verifica que $o(g_j) = o(h_j)$ para $j = 1, \ldots, n$. Es decir, $G = \langle g_1 \rangle \times \cdots \times \langle g_n \rangle$, con $\operatorname{ord}(g_1) \geq \cdots \geq \operatorname{ord}(g_n)$, y la n-tupla $(\operatorname{ord}(g_1), \ldots, \operatorname{ord}(g_n))$ queda determinada de manera única por G.

Demostración. La existencia de tal descomposición es una consecuencia inmediata del lema 6.4.2. Para ello se inicia con un elemento g_1 de orden maximal en G y luego aplica la hipótesis al complemento U.

Para demostrar la unicidad de la descomposición, enumeremos los g_j de tal manera que $\operatorname{ord}(g_j) = p^{a_j}$ con

$$a_1 \geq \cdots \geq a_k > a_{k+1} = \cdots = a_n = 1.$$

Si consideramos nuevamente el endomorfismo de G definido por $\varepsilon(x) := x^p$, entonces

$$\operatorname{Im}(\varepsilon) = \langle g_1^p \rangle \times \cdots \times \langle g_n^p \rangle = \langle g_1^p \rangle \times \cdots \times \langle g_k^p \rangle$$

y además $|\operatorname{Im}(\varepsilon)| = p^{a_1 - 1} \cdots p^{a_k - 1}$, con lo cual se tiene que $|G/\operatorname{Im}(\varepsilon)| = p^n$. Un argumento similar con los h_j demuestra que $|G/\operatorname{Im}(\varepsilon)| = p^m$ y así, $m = n$.

Usando inducción matemática sobre $|G|$ se demuestra que los k números $a_1 - 1, \ldots, a_k - 1$ quedan determinados de manera única por $\operatorname{Im}(\varepsilon)$ y, por lo tanto, también por G. Dado que n queda determinado por $G/\operatorname{Im}(\varepsilon)$, los exponentes $a_1, \ldots, a_n$ quedan determinados de manera única por G. □

El siguiente teorema suministra una clasificación completa de los grupos abelianos finitos. Demostramos que si G es un grupo abeliano finito, entonces G es isomorfo a un producto directo de grupos cíclicos cuyos ordenes son potencias de números primos.

6.4.4 Teorema fundamental sobre grupos abelianos finitos. Sea $1 \neq G$ un grupo abeliano finito. Entonces G es un producto directo de subgrupos cíclicos no triviales cuyos órdenes son potencias de números primos.

Demostración. Del teorema 6.2.10 se sigue que G es producto directo de sus subgrupos de Sylow, $P_1, \ldots, P_k$. Es decir, $G = P_1 \times \cdots \times P_k$. La existencia de una descomposición de la forma

$$G = \langle g_1 \rangle \times \cdots \times \langle g_n \rangle \tag{6.10}$$

se sigue del teorema 6.4.3.

Si p_j es un divisor de $|G|$, entonces del corolario 6.2.8 se sigue que los p_j-subgrupos de Sylow P_j de G contienen exactamente los elementos de G, cuyos órdenes son p_j-potencias.

Sean $U_{j1}, \ldots, U_{jn_j}$ los factores en (6.10) para los cuales $p_j \mid |U_{ji}|$. Entonces se sigue que

$$|U_{j1} \times \cdots \times U_{jn_j}| = |P_j|$$

y, en consecuencia, $U_{j1} \times \cdots \times U_{jn_j} = P_j$. $\square$

6.4.5 Definición. Sea $G = \langle g_1 \rangle \times \cdots \times \langle g_n \rangle$ un grupo abeliano finito, con $\operatorname{ord}(g_j) = p_j^{a_j}$, donde cada p_j es un número primo y $a_j \in \mathbb{N}$. Ordenamos los p_j de menor a mayor y para dos primos iguales, digamos $p_j = p_{j+1}$, se cuenta primero la mayor potencia de p_j. Es decir,

$$p_1 \leq p_2 \leq \ldots \leq p_n$$

y si $p_j = p_{j+1}$, entonces $a_j \geq a_{j+1}$. Entonces

(1) La n-tupla $(p_1^{a_1}, \ldots, p_n^{a_n})$ formada con este orden y según el teorema fundamental de los grupos abelianos, determinada de manera única por el grupo G, se denomina `el tipo` de G.

Dado que $\langle g_j \rangle \cong \mathbb{Z}_{p_j^{a_j}}$ para todo $j = 1, \ldots, n$, se sigue que $G \cong \mathbb{Z}_{p_1^{a_1}} \times \cdots \times \mathbb{Z}_{p_n^{a_n}}$. En consecuencia, todo grupo abeliano finito queda completamente determinado por su tipo.

(2) Un p-grupo abeliano finito del tipo $(p, p, \ldots, p)$ se denomina `abeliano elemental`.

6.4.6 Ejemplo. Salvo isomorfía existen nueve grupos abelianos de orden $1000 = 2^3 5^3$, como se muestra en la siguiente tabla:

Grupo	Tipo
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5$	$(2, 2, 2, 5, 5, 5)$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{5^2} \times \mathbb{Z}_5$	$(2, 2, 2, 5^2, 5)$
$\mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5$	$(2^2, 2, 5, 5, 5)$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{5^3}$	$(2, 2, 2, 5^3)$
$\mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_{5^2} \times \mathbb{Z}_5$	$(2^2, 2, 5^2, 5)$
$\mathbb{Z}_{2^3} \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5$	$(2^3, 5, 5, 5)$
$\mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_{5^3}$	$(2^2, 2, 5^3)$
$\mathbb{Z}_{2^3} \times \mathbb{Z}_{5^2} \times \mathbb{Z}_5$	$(2^3, 5^2, 5)$
$\mathbb{Z}_{2^3} \times \mathbb{Z}_{5^3}$	$(2^3, 5^3)$

Tabla 6.1: Grupos abelianos de orden 1000

6.4.7 Observación. En la siguiente tabla presentamos una clasificación de todos los grupos, salvo isomorfía, hasta el orden 15.

$\|G\|$	Grupos abelianos	Grupos no abelianos
1	1	
2	$\mathbb{Z}_2$	
3	$\mathbb{Z}_3$	
4	$\mathbb{Z}_4,\ \mathbb{Z}_2 \times \mathbb{Z}_2$	
5	$\mathbb{Z}_5$	
6	$\mathbb{Z}_6$	$\mathrm{Sym}(3)$
7	$\mathbb{Z}_7$	
8	$\mathbb{Z}_8,\ \mathbb{Z}_4 \times \mathbb{Z}_2,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	D_8, $\mathbb{Q}_8$
9	$\mathbb{Z}_9,\ \mathbb{Z}_3 \times \mathbb{Z}_3$	
10	$\mathbb{Z}_{10}$	D_{10}
11	$\mathbb{Z}_{11}$	
12	$\mathbb{Z}_{12},\ \mathbb{Z}_2 \times \mathbb{Z}_6$	$\mathrm{Alt}(4),\ D_{12},\ \mathbb{Z}_4 \rtimes \mathbb{Z}_3$
13	$\mathbb{Z}_{13}$	
14	$\mathbb{Z}_{14}$	D_{14}
15	$\mathbb{Z}_{15}$	

Tabla 6.2: Clasificación de los grupos hasta orden 15

Presentamos a continuación una consecuencia importante del teorema fundamental para los grupos abelianos finitos. Esta propiedad se tenía hasta el momento solo para grupos cíclicos.

6.4.8 Corolario. Si G es un grupo abeliano finito y d un divisor de $|G|$, entonces existe $U \leq G$ con $|U| = d$.

Demostración. Si $|G| = n_1 \cdots n_r$, entonces $G \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$. Si d divide a $|G|$, entonces existen d_j con $d_j \mid n_j$, $(j = 1, \ldots, r)$ tales que $d = d_1 \cdots d_r$. Por lo tanto, $\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_r}$ es isomorfo a un subgrupo de G con orden d. □

6.4.9 Observación. Existe una versión general del teorema fundamental de los grupos abelianos finitos. En efecto, todo grupo abeliano finitamente generado es producto directo de subgrupos cíclicos. Una demostración de este resultado puede verse, por ejemplo, en [7] teorema 4.J. p. 191.

6.5 Ejercicios

1. Sea V un espacio vectorial sobre un cuerpo K. Demuestre que el grupo multiplicativo $K^\times$ actúa sobre V mediante $\lambda \cdot v := \lambda v$ para todo $\lambda \in K^\times$ y $v \in V$. Determine además las órbitas de esta acción.

2. Sean $\Omega = \{1, \ldots, n\}$ y $G = \mathrm{Sym}(\Omega)$. Si para $\omega \in \Omega$ y $\sigma \in G$ definimos la acción $\sigma \cdot \omega := \sigma(\omega)$, demuestre que Ω es un G-conjunto.

3. Sea V un espacio vectorial de dimensión 3 sobre el cuerpo binario $\mathbb{F}_2$. Consideremos el grupo $G = GL(V)$ y sea $\Omega := V \setminus \{0\}$. Demuestre que

   (a) $|\Omega| = 7$ y $|G| = 168$.

   (b) G actúa transitivamente sobre Ω.

   (c) G admite un subgrupo U de índice 7.

   (d) Si N es un subgrupo normal propio de G, entonces U no es subgrupo de N.

   (e) $G = UN$ y 7 divide a $|N|$.

4. Para cada uno de los grupos $\mathrm{Sym}(3), \mathbb{Q}_8, D_8$ y $\mathrm{Alt}(4)$ determine

   (a) la ecuación de clases,

   (b) los centralizadores de sus subgrupos.

5. Demuestre que si un grupo G de orden 6 tiene un subgrupo no normal H con orden 2, entonces G es isomorfo a $\mathrm{Sym}(3)$.

6. Sean Ω_1 y Ω_2 dos G-conjuntos. Decimos que estos son isomorfos, como G-conjuntos, si existe una biyección $\alpha : \Omega_1 \longrightarrow \Omega_2$ con $\alpha(g \cdot \omega) = g \cdot \alpha(\omega)$ para todo $g \in G$ y todo $\omega \in \Omega_1$. Demuestre que si Ω_1 es un G-conjunto transitivo, $\omega \in \Omega_1$ y $U = G_\omega$, entonces Ω_1 es isomorfo a $\Omega_2 := \{gU \mid g \in G\}$.

7. Sea G un grupo finito. Si $U \leq G$ con $|G : U| = n$, entonces G tiene un subgrupo normal N tal que n divide a $|G : N|$ y $|G : N|$ divide a $n!$

8. Los grupos $\mathrm{Sym}(4)$ y $\mathrm{Alt}(4)$ operan transitivamente (por conjugación) sobre el 4-grupo de Klein $V_4 = \{(1), (12)(34), (13)(24), (14)(23)\}$. Determine el estabilizador de $\omega = (12)(34)$ bajo las dos operaciones.

9. Si $G = \mathrm{Sym}(4)$, calcule $N_G(V_4)$, $C_G((1\ 2)(3\ 4))$.

10. Sea G un grupo, $M \subseteq G$, $g \in G$ y $U \leq G$. Demuestre que $C_U(g) = C_G(g) \cap U$.

11. Sea $G = \mathrm{Sym}(4)$, $g = (1234)$ y $h = (2314) \in G$.

(a) Determine el número de elementos $x \in G$ tales que $x^{-1}gx = h$.

(b) Calcule $C_G(g)$ y $N_G(\langle g \rangle)$.

12. Si G es un grupo abeliano y $k \in \mathbb{Z}$, definimos $G^k := \{g^k \mid g \in G\}$. Decimos que k `aniquila a` G si $G^k = 1$. Demuestre que el conjunto

$$K(G) := \{k \mid k \text{ aniquila a } G\}$$

es un subgrupo de $\mathbb{Z}$ y, por lo tanto, es de la forma $m\mathbb{Z}$ para algún $m \in \mathbb{N}_0$. Este número m es denominado el `exponente` de G y lo notamos con $\mathrm{Exp}(G)$.

13. Demuestre que $\mathrm{Exp}(\mathbb{Z}) = 0$, $\mathrm{Exp}(\mathbb{Z}_n) = n$, $\mathrm{Exp}(V_4) = 2$ y $\mathrm{Exp}(\mathrm{Sym}(3)) = 6$.

14. Sea G un grupo abeliano con $\mathrm{Exp}(G) = m$. Demuestre que

(a) Para todo entero k, k aniquila a G si y solo si $m \mid k$.

(b) Si G es finito, entonces $m \mid |G|$.

(c) Si $m \neq 0$, entonces para todo $g \in G$ se verifica que $\mathrm{ord}(g) \mid m$.

(d) Si G es cíclico, entonces

$$\mathrm{Exp}(G) = \begin{cases} 0 & \text{si } G \text{ es infinito} \\ |G| & \text{si } G \text{ es finito} \end{cases}$$

15. Demuestre que si G es un grupo finito, entonces

$$\mathrm{Exp}(G) := \mathrm{mcm}\{\mathrm{ord}(g) \mid g \in G\}.$$

16. Demuestre que todo grupo G con $\mathrm{Exp}(G) = 2$ es abeliano.

17. Sea G un grupo abeliano y $g \in G$. Supóngase que para algún primo p y algún entero a se verifica que $g^{p^{a-1}} \neq 1$ y $g^{p^a} = 1$. Demuestre que $\mathrm{ord}(g) = p^a$.

18. Sea G un grupo abeliano con $\mathrm{Exp}(G) = m \neq 0$. Demuestre que G tiene un elemento de orden m.

19. Sea G un grupo abeliano finito y $n \in \mathbb{N}$. Demuestre que si $n \mid \mathrm{Exp}(G)$, entonces existe $h \in G$ tal que $\mathrm{ord}(h) = n$.

20. Sea G un grupo abeliano finito y $N \leq G$. Demuestre que $\mathrm{Exp}(G/N)$ divide a $\mathrm{Exp}(G)$.

21. Sea G un grupo abeliano finito y p un número primo con $p \mid |G|$. Demuestre que $p \mid \mathrm{Exp}(G)$, y en particular que existe $g \in G$ tal que $\mathrm{ord}(g) = p$.

22. Sea G un grupo abeliano finito. Demuestre que los números primos que dividen a $\mathrm{Exp}(G)$ son los mismos primos que dividen a $|G|$.

23. Si G un grupo abeliano finito tal que $|G| = mn$, con $m, n \in \mathbb{N}$ y $\text{mcd}(m,n) = 1$. Entonces existen $U, V \leq G$ con $G = U \times V$, $|U| = m$ y $|V| = n$.

24. Sea G un grupo, p un número primo, P un p-subgrupo de G, $N \trianglelefteq G$ y $p \nmid |N|$. Demuestre que

    (a) $N_G(P)N/N = N_{G/N}(PN/N)$.

    (b) $C_G(P)N/N = C_{G/N}(PN/N)$.

25. Sea G un grupo finito tal que $|G| = pq$, donde $p > q$ (números primos) y además q no divide a $p-1$. Demuestre que G es un grupo cíclico.

26. Demuestre que ningún grupo con orden 12, 20, 28, 42, 48, 56, 130, 132, 255, 300, 312 o 1000 es simple.

27. Sea G un grupo tal que $|G| = 2p$, donde p es un primo impar. Demuestre que G no es simple.

28. Sean p y q dos números primos distintos. Determine todos los grupos abelianos, salvo isomorfá con orden $p^a q^b$, donde $a, b \in \mathbb{N}$.

29. Clasifique, salvo isomorfía, todos los grupos abelianos de orden 16 y de orden 200.

30. Sea G un grupo de orden 12.

    (a) ¿Cuáles números son posible para $|\text{Syl}_2(G)|$ y $|\text{Syl}_3(G)|$?

    (b) Demuestre que no es posible que simultaneamente $|\text{Syl}_2(G)| = 3$ y $|\text{Syl}_3(G)| = 4$.

    (c) Demuestre que si $|\text{Syl}_2(G)| = |\text{Syl}_3(G)| = 1$, entonces G es un grupo abeliano.

31. Demuestre que si todos los subgrupos de Sylow de un grupo G son normales, entonces G es el producto directo (interno) de estos.

32. Sea G un grupo abeliano, con $|G| = mn$, donde m y n son números primos distintos. Demuestre que G es cíclico. ¿Se verifica la afirmación si $m = n$?

33. Determine todas las clases de conjugación de $\text{Sym}(3)$.

34. Determine los 2-subgrupos de Sylow del 4-grupo de Klein.

35. Presente una acción no transitiva de un grupo sobre un conjunto.

36. Sea G un grupo, Ω un G-conjunto y $\alpha : G \longrightarrow \text{Sym}(\Omega)$, definida por

$$G \ni g \overset{\alpha}{\longmapsto} (\omega \longmapsto g \circ \omega) \in \text{Sym}(\Omega).$$

    (a) Si $K := \mathcal{N}(\alpha)$, entonces Ω es un G/K-conjunto si definimos $(gK) \circ \omega := g \circ \omega$.

(b) Si Ω es un G-conjunto transitivo, entonces Ω es un G/K-conjunto transitivo.

(c) Si Ω es un G-conjunto transitivo, entonces $|K| \leq \frac{|G|}{|\Omega|}$.

37. Sea G un grupo tal que $|G| = 2p$, donde p es un primo impar. Demuestre que G no es simple.

38. Sea G un p-grupo abeliano elemental, con orden p^n. Demuestre que $\mathrm{Aut}(G)$ es isomorfo al grupo aditivo del espacio vectorial $\mathbb{Z}_p^n$.

39. ¿Es $(\mathbb{Q}, +)$ un grupo finitamente generado?

40. El grupo $\mathrm{Alt}(4)$ opera transitivamente (por conjugación) sobre el grupo $V4 = \{(1), (12)(34), (13)(24), (14)(23)\}$. Determine el estabilizador de $\omega = (12)(34)$ bajo esta operación.

41. Sea $|G| = p^2q$, con $p \neq q$. Demuestre que G admite bien un p-subgrupo de Sylow normal o un q-subgrupo de Sylow normal.

42. Halle todos los p-subgrupos de Sylow de $\mathrm{Alt}(4)$ y demuestre que $\mathrm{Alt}(4)$ no tiene subgrupos de índice 6.

43. Demuestre que existe, salvo isomorfía, un único grupo simple con orden 60, concretamente $\mathrm{Alt}(5)$.

44. Sea G un grupo finito. Demuestre que si la intersección de cualquier par de p-subgrupos de Sylow de G es trivial, entonces

$$|\{g \in G \mid \mathrm{ord}(g) = p^a, \text{con } a \geq 1\}| = |\mathrm{Syl}_p(G)|(|P| - 1),$$

donde $P \in \mathrm{Syl}_p(G)$.

45. Sea $G = \langle g_1 \rangle \times \cdots \times \langle g_n \rangle$ un grupo abeliano elemental. Es decir, G es un p-grupo abeliano del tipo $(p, p, \ldots, p)$ y $\mathrm{ord}(g_j) = p$ para todo $j = 1, 2, \ldots, n$. Denotemos con $V(n, p)$ el espacio vectorial de dimensión n sobre $\mathrm{GF}(p)$, el campo de Galois de orden p y sea $V(n, p)^+$ su grupo aditivo. Demuestre que

(a) La función $\varepsilon : G \longrightarrow V(n, p)^+$ definida por

$$\varepsilon(g_1^{\alpha_1}, \ldots, g_n^{\alpha_n}) := (\alpha_1 + p\mathbb{Z}, \ldots, \alpha_n + p\mathbb{Z})$$

es un isomorfismo.

(b) Si $\alpha \in \mathrm{Aut}(G)$ con $\alpha(g_1^{\alpha_1}, \ldots, g_n^{\alpha_n}) = (g_1^{\alpha'_1}, \ldots, g_n^{\alpha'_n})$, entonces la función $\tau : \mathrm{Aut}(G) \longrightarrow \mathrm{GL}_n(p)$ definida por

$$\tau(\alpha)(\alpha_1 + p\mathbb{Z}, \ldots, \alpha_n + p\mathbb{Z}) := (\alpha'_1 + p\mathbb{Z}, \ldots, \alpha'_n + p\mathbb{Z})$$

es un isomorfismo. Es decir, se verifica que $\mathrm{Aut}(G) \cong \mathrm{GL}_n(p)$.

CAPÍTULO 7

GRUPOS SOLUBLES

A los matemáticos les es habitual pretender que las ideas de que se ocupan son de naturaleza tan refinada y espiritual que no son del dominio de la fantasía, sino que deben ser comprendidas por una visión pura e intelectual de la que sólo las facultades del alma son capaces.
(Tratado de la Naturaleza Humana - David Hume)

A lo largo de este capítulo G denota siempre un grupo.

7.1 Conmutadores y el subgrupo derivado

En el primer capítulo se introdujo el concepto de centro de un grupo. Este nos permite tener una "medida" de la conmutatividad de la operación en el grupo. En efecto, un grupo que coincide con su centro es abeliano. Por el contrario, un grupo con centro propio indica automáticamente que el grupo no es abeliano.

Otro concepto importante asociado a la conmutatividad de un grupo es el de grupo conmutador. Con este podemos también determinar en qué medida un grupo no es abeliano.

7.1.1 Definición. Sean $g, h \in G$ y $U, V \leq G$.

(1) Definimos el `conmutador` de g con h, notado $[g, h]$ así:

$$[g, h] := g^{-1}h^{-1}gh.$$

(2) Se define y nota el conmutador de U con V de la siguiente manera:

$$[U,V] \coloneqq \langle [u,v] \mid u \in U, v \in V \rangle .$$

En particular, $[G,G]$ se nota con G' y se denomina el `grupo conmutador` o `derivado` de G.

(3) La `clausura normal` de U en G, notada con $\langle U^G \rangle$, se define así.

$$\langle U^G \rangle \coloneqq \langle U^g \mid g \in G \rangle.$$

Resulta evidente que la clausura normal de U en G es el subgrupo normal más pequeño de G que contiene a U.

7.1.2 Observaciones. (1) $[g,h] = 1$ si y solo si $gh = hg$.

(2) Si $U, V \leq G$, entonces $[U,V] \leq G$.

(3) Si $A \leq U$, $B \leq V$, entonces $[A,B] \leq [U,V]$.

7.1.3 Ejemplos. (1) Si G es abeliano, entonces $G' = 1$.

(2) Consideremos el grupo $\mathbb{Q}_8$ de los cuaterniones. Recordemos que

$$\begin{aligned} \mathbb{Q}_8 &= \langle x, y \mid x^4 = 1,\ (xy)^2 = x^2 = y^2,\ yxy^{-1} = x^{-1} \rangle. \\ &= \{1, x, x^2, x^3, y, xy, x^2y, x^3y\} \\ &= \{x^m y^n \mid m = 0,1,2,3, \text{ y } n = 0,1\}. \end{aligned}$$

Demostramos que $[\mathbb{Q}_8, \mathbb{Q}_8] = \langle x^2 \rangle$.

Note inicialmente que

$$[x^m y^n, x^r y^j] = y^{-n} x^{-m} y^{-j} x^{m-r} y^n x^r y^j.$$

Diferenciamos todos los casos posibles:

Caso 1. Si $n = j = 0$, entonces $[x^m y^n, x^r y^j] = [x^m, x^r] = 1$.

Caso 2. Si $n = 1$ y $j = 0$, entonces

$$\begin{aligned} [x^m y^n, x^r y^j] &= y^{-1} x^{-m} x^{m-r} y x^r \\ &= y^{-1} x^{-r} y x^r \\ &= y^{-1} y x^r x^r \\ &= x^{2r} \\ &= (x^2)^r \in \langle x^2 \rangle. \end{aligned}$$

Caso 3. Si $n = 0$ y $j = 1$, entonces

$$\begin{aligned}[x^m y^n, x^r y^j] &= x^{-m} y^{-1} x^{m-r} x^r y \\ &= x^{-m} y^{-1} x^m y \\ &= x^{-m} x^{-m} y^{-1} y \\ &= x^{-2m} \\ &= (x^{-2})^m \\ &= (x^2)^m \in \langle x^2 \rangle.\end{aligned}$$

Caso 4. Si $n = j = 1$, entonces

$$\begin{aligned}[x^m y^n, x^r y^j] &= y^{-1} x^{-m} y^{-1} x^{m-r} y x^r y \\ &= x^m y^{-1} y^{-1} x^{m-r} y x^r y \\ &= x^m y^{-2} x^{m-r} y x^r y \\ &= x^m x^2 x^{m-r} y x^r y \\ &= x^{2m-r+2} y x^r y \\ &= x^{2m-r+2} x^{-r} y y \\ &= x^{2m-2r+2} x^2 \\ &= (x^2)^{m-r} \in \langle x^2 \rangle.\end{aligned}$$

Esto demuestra que $[\mathbb{Q}_8, \mathbb{Q}_8] \subseteq \langle x^2 \rangle$.

Recíprocamente, note que

$$[x, xy] = x^{-1} y^{-1} x^{-1} x x y = x^{-1} y^{-1} x y = x^{-1} x^{-1} y^{-1} y = x^{-2} = x^2.$$

Esto demuestra que $x^2 \in [\mathbb{Q}_8, \mathbb{Q}_8]$ y, en consecuencia, $\langle x^2 \rangle \subseteq [\mathbb{Q}_8, \mathbb{Q}_8]$, con lo cual se tiene la afirmación.

7.1.4 Lema. Sean $g, h, k \in G$. Entonces

(1) $[g, h]^{-1} = [h, g]$

(2) $[g^k, h^k] = [g, h]^k$

(3) $[g, hk] = [g, k][g, h]^k$

(4) $[gh, k] = [g, k]^h [h, k]$.

Demostración. Se deja como ejercicio. □

7.1.5 Lema. Sean $U, V \leq G$. Entonces

(1) $[U,V] = [V,U] \trianglelefteq \langle U,V\rangle$.

(2) $[U,V] \leq U$ si y solo si $V \leq N_G(U)$.

(3) Si $\alpha : G \longrightarrow \alpha(G)$ es un homomorfismo, entonces

$$\alpha([U,V]) = [\alpha(U), \alpha(V)].$$

Si U, V char G, entonces $[U,V]$ char G. En particular G' char G.

(4) Si $U, V \trianglelefteq G$, entonces $[U,V] \trianglelefteq G$ y $[U,V] \leq U \cap V$.

Demostración. (1) Sea $x \in [U,V]$. Entonces $x = [u_1, v_1]^{\epsilon_1} \cdots [u_n, v_n]^{\epsilon_n}$, con $u_j \in U$, $v_j \in V$, $\epsilon_j \in \mathbb{Z}$, $n \in \mathbb{N}$. Dado que $[u_j, v_j] = [v_j, u_j]^{-1}$ para todo j, se sigue que $x \in [V,U]$. Es decir, $[U,V] \subseteq [V,U]$. Similar se demuestra la otra contenencia.

Para demostrar que $[U,V]$ es normal en $\langle U,V\rangle$, sean $x \in [U,V]$ y $z \in \langle U,V\rangle$. Una vez mas se tiene que $x = [u_1, v_1]^{\epsilon_1} \cdots [u_n, v_n]^{\epsilon_n}$, con $u_j \in U$, $v_j \in V$, $\epsilon_j \in \mathbb{Z}$, $n \in \mathbb{N}$ y $z = z_1^{\tau_1} \cdots z_m^{\tau_m}$, con $z_j \in U \cup V$, $\tau_j \in \mathbb{Z}$, $m \in \mathbb{N}$. Para demostrar que $z^{-1}xz \in [U,V]$ es suficiente demostrar que $[u_j, v_j]^{z_j}$ y $[u_j, v_j]^{z_j} \in [U,V]$ para $z_j \in U$ o $z_j \in V$.

Si $z_j \in V$, entonces del lema 7.1.4 (3) se sigue que

$$[u_j, v_j]^{z_j} = [u_j, z_j]^{-1} [u_j, v_j z_j] \in [U,V]$$

y si $z_j \in U$, entonces del lema 7.1.4 (4)

$$[u_j, v_j]^{z_j} = [u_j z_j, v_j][z_j, v_j]^{-1} \in [U,V].$$

Por lo tanto, $[U,V] \trianglelefteq \langle U,V\rangle$.

(2) Sean $u \in U$ y $v \in V$. Note que $[u,v] = u^{-1}v^{-1}uv = u^{-1}u^v$. Por lo tanto,

$$\begin{aligned} [u,v] \in U &\iff u^v \in U \\ &\iff v \in N_G(U) \\ &\iff V \leq N_G(U). \end{aligned}$$

En consecuencia, $[U,V] \leq U$ si y solo si $V \leq N_G(U)$.

(3) Sea α un epimorfismo. Entonces

$$\begin{aligned} \alpha([U,V]) &= \alpha(\langle [u,v] \mid u \in U, v \in V\rangle) \\ &= \langle \alpha([u,v]) \mid u \in U, v \in V\rangle \\ &= \langle [\alpha(u), \alpha(v)] \mid u \in U, v \in V\rangle \\ &= [\alpha(U), \alpha(V)]. \end{aligned}$$

(4) Si $U, V \trianglelefteq G$, entonces $[U,V] \trianglelefteq G$, ya que en (3) podemos hacer que α recorra el grupo de los automorfismos interiores.

Por otro lado, dado que $U, V \trianglelefteq G$, se tiene que $N_G(V) = N_G(U) = G$. Usando (2) se sigue simultáneamente que $[U,V] \leq U$ y $[U,V] \leq V$ y se tiene que $[U,V] \leq U \cap V$. □

7.1.6 Lema. Sea G un grupo. Si $N \trianglelefteq G$, entonces $[G/N, G/N] = G'N/N$.

Demostración. Si $N \trianglelefteq G$, entonces

$$\begin{aligned}[G/N, G/N] &= \langle [gN, hN] \mid g, h \in G \rangle \\ &= \langle [g,h]N \mid g, h \in G \rangle \\ &= G'N/N,\end{aligned}$$

con lo cual se tiene la afirmación. □

7.1.7 Lema. (1) Si $G' \leq N \leq G$, entonces $N \trianglelefteq G$.

(2) G/G' es abeliano.

(3) Si $N \trianglelefteq G$ y G/N es abeliano, entonces $G' \subseteq N$. En particular $|G : G'| \geq |G : N|$ para todo $N \trianglelefteq G$, con G/N abeliano.

Demostración. (1) Si $G' \leq N \leq G$, entonces $[G,N] \leq [G,G] = G' \leq N$. Usando el lema 7.1.5 (2) se sigue que $G \leq N_G(N)$. Es decir, $N_G(N) = G$, por lo tanto, $N \trianglelefteq G$.

(2) Sean $xG', yG' \in G/G'$. Entonces

$$\begin{aligned}x^{-1}G'y^{-1}G'xG'yG' &= x^{-1}y^{-1}xyG' \\ &= [x,y]G' \\ &= G'.\end{aligned}$$

Esto trae como consecuencia que $xG'yG' = yG'xG'$, y así G/G' es abeliano.

(3) Sea $N \trianglelefteq G$, con G/N abeliano. Entonces $[G/N, G/N] = 1$. Usando el lema anterior tenemos:

$$\begin{aligned}[G/N, G/N] = 1 &\Leftrightarrow G'N/N = 1 \\ &\Leftrightarrow G'N = N \\ &\Leftrightarrow G' \leq N.\end{aligned}$$

Finalmente, del teorema de Lagrange se sigue que $|G| = |G : N||N| \geq |G : N||G'|$. Por lo tanto, $|G : G'||G'| = |G| \geq |G : N||G'|$. Esto implica que $|G : G'| \geq |G : N|$, con lo cual se completa la prueba. □

7.1.8 Ejemplo. Sea $n \in \mathbb{N}$. Entonces

(1) $\mathrm{Sym}(n)' = \mathrm{Alt}(n)$.

Los casos $n = 1$ y $n = 2$ son inmediatos. Supongamos que $n \geq 3$. Demostramos inicialmente que todo 3-ciclo pertenece a $\mathrm{Sym}(n)'$. En efecto, sean $a, b, c \in \{1, \ldots, n\}$ distintos. Entonces

$$(abc) = (ac)(cb)(ac)(cb) = [(ac), (cb)].$$

Dado que $\mathrm{Alt}(n)$ es generado por los 3-ciclos, se tiene que $\mathrm{Alt}(n) \subseteq \mathrm{Sym}(n)'$.

Recíprocamente, dado que $\mathrm{Alt}(n) \trianglelefteq \mathrm{Sym}(n)$ y $\mathrm{Sym}(n)/\mathrm{Alt}(n)$ es abeliano, del lema anterior se sigue que $\mathrm{Sym}(n)' \subseteq \mathrm{Alt}(n)$.

(2) $\mathrm{Alt}(n)' = \mathrm{Alt}(n)$ si $n \geq 5$.

Es conocido que para $n \geq 5$ el grupo $\mathrm{Alt}(n)$ no es abeliano y además es simple. Dado que $\mathrm{Alt}(n)' \trianglelefteq \mathrm{Alt}(n)$, se sigue que $\mathrm{Alt}(n)' = \mathrm{Alt}(n)$.

7.1.9 Lema. Sean $H, K \leq G$. Entonces $\langle H^k \mid k \in K \rangle = \left\langle \bigcup_{k \in K} H^k \right\rangle = H[H, K]$.

Demostración. Del lema 7.1.5 (1) se sigue que $[H, K] \trianglelefteq \langle H, K \rangle$. Por lo tanto, $H[H, K] = [H, K]H$, y se tiene, en consecuencia, que $H[H, K]$ es un subgrupo de G.

Por otro lado para todo $h \in H$ y $k \in K$ se verifica que

$$h^k = k^{-1}hk = h[h, k] \in H[H, K].$$

Entonces

$$\langle H^k \mid k \in K \rangle = \Big\langle \bigcup_{k \in K} H^k \Big\rangle \leq H[H, K].$$

Además, dado que H y $[H, K]$ son claramente subgrupos de $\langle H^k \mid k \in K \rangle$ y se tiene que $H[H, K] \leq \langle H^k \mid k \in K \rangle$, con lo cual se tiene la igualdad.

7.1.10 Lema. Sean $U, H, K \leq G$. Si $U \leq N_G(H) \cap N_G(K)$, entonces

$$[HU, K] = [H, K][U, K].$$

Demostración. En primer lugar es necesario controlar que $[H, K][U, K]$ es un subgrupo de G. Dado que $U \leq N_G(H)$, se tiene que $H^u = H$ para todo $u \in U$. Esto es equivalente a decir que $uH = Hu$ para todo $u \in U$. O, equivalentemente, $HU = UH$, la cual es una condición necesaria y suficiente para que HU sea un subgrupo de G.

Por otro lado,

$$[HU, K] = \langle [hu, k] \mid h \in H, u \in U, k \in K \rangle.$$

Del lema 7.1.5 (1) se sigue que $[H,K] \trianglelefteq \langle H,K\rangle$, y dado que $U \leq N_G(K)$, usando nuevamente el lema 7.1.5 (2) tenemos que $[U,K] \leq K$. En resumen, se tiene

$$[U,K] \leq K \leq N_G([H,K]).$$

Similar como antes, podemos afirmar que $[H,K][U,K]$ es un subgrupo de G.

Note ahora que si $h \in H$, $u \in U$ y $k \in K$, entonces del lema 7.1.4 se tiene que

$$[hu,k] = [h,k]^u[u,k] = [h^u,k^u][u,k] \in [H,K][U,K],$$

ya que U normaliza tanto a H como a K. Esto demuestra que $[HU,K] \leq [H,K][U,K]$.

Recíprocamente, del hecho que $H,U \leq HU$ se sigue la otra contenencia. □

7.1.11 Teorema. Sean $N,M \trianglelefteq G$. Entonces $G/(N \cap M)$ es isomorfo a un subgrupo de $G/M \times G/N$.

Demostración. Consideremos la función $\varphi : G \longrightarrow G/M \times G/N$ definida por

$$\varphi(g) := (gM, gN).$$

φ `es homomorfismo.` Sean $g,h \in G$. De la definición de producto directo se sigue que

$$\begin{aligned}\varphi(gh) &= (ghM, ghN)\\ &= (gMhM, gNhN)\\ &= (gM,gN)(hM,hN)\\ &= \varphi(g)\varphi(h).\end{aligned}$$

Por otro lado,

$$g \in \ker(\varphi) \Leftrightarrow (gM,gN) = (M,N) \Leftrightarrow g \in M \cap N.$$

Aplicando el primer teorema de isomorfía se tiene que

$$G/(M \cap N) \cong \varphi(G) \leq G/M \times G/N.$$

□

7.2 Derivados de orden superior

7.2.1 Definición. De manera recursiva definimos los subgrupos `derivados de orden superior` de G. Para $n \in \mathbb{N}_0$

$$G^{(0)} := G$$
$$G^{(1)} := G'$$
$$G^{(n+1)} := (G^{(n)})' = [G^{(n)}, G^{(n)}].$$

Si $G' = G$, entonces G se denomina `perfecto`. Note que se tiene la cadena

$$G = G^{(0)} \geq G^{(1)} \geq G^{(2)} \geq \cdots$$

Definimos

$$G^{(\infty)} := \bigcap_{j \in \mathbb{N}} G^{(j)}.$$

7.2.2 Ejemplos. (1) Todo grupo no abeliano simple es perfecto.

(2) El grupo $\mathrm{Alt}(5)$ es perfecto. Usando, por ejemplo, el software GAP se encuentra que $\mathrm{Alt}(5)' = \langle (132), (243), (23)(45) \rangle$ y tiene orden 60.

(3) El grupo lineal especial $\mathrm{SL}_2(5)$ de las matrices de tamaño 2×2 sobre $\mathbb{Z}_5$ con determinante 1 no es simple y es perfecto. Usando GAP se verifica que $|\mathrm{SL}_2(5)| = 120$.

7.2.3 Lema. Sea G y H grupos, $U \leq G$, $N \trianglelefteq G$ y $n \in \mathbb{N}_0$. Entonces

(1) $U^{(n)} \leq G^{(n)}$.

(2) $(G/N)^{(n)} = G^{(n)}N/N$.

(3) $\alpha(G^{(n)}) = \alpha(G)^{(n)}$ para todo $\alpha \in \mathrm{Hom}(G, H)$. En particular se tiene que $G^{(n)}$ es un subgrupo de G completamente invariante.

(4) $(G \times H)^{(n)} = G^{(n)} \times H^{(n)}$.

Demostración. (1) Procedemos por inducción sobre n. Si $n = 0$, entonces la afirmación es inmediata. Supongamos que $U^{(n)} \leq G^{(n)}$. Entonces

$$U^{(n+1)} = [U^{(n)}, U^{(n)}] \leq [G^{(n)}, G^{(n)}] = G^{(n+1)}.$$

(2) Procedemos por inducción sobre n. Si $n = 0$, entonces la afirmación es inmediata. Como hipótesis de inducción supongamos válido que

$$(G/N)^{(n)} = G^{(n)}N/N.$$

Del lema 7.1.6 se tiene que $(G/N)' = G'N/N$. Entonces

$$\begin{aligned}(G/N)^{(n+1)} &= ((G/N)^{(n)})' \\ &= (G^{(n)}N/N)' \\ &= (G^{(n)}N)'N/N \\ &\geq (G^{(n)})'N/N \\ &= G^{(n+1)}N/N.\end{aligned}$$

Para demostrar la otra inclusión tenemos

$$(G/N)^{(n+1)} = (G^{(n)}N)'N/N = [G^{(n)}N, G^{(n)}N]N/N.$$

Por otro lado, note que $G^{(n)}$, N y $G^{(n)}N$ son subgrupos normales de G y podemos usar repetidamente el lema 7.1.10 para obtener

$$\begin{aligned}[G^{(n)}N, G^{(n)}N] &= [G^{(n)}, G^{(n)}N][N, G^{(n)}N] \\ &= [G^{(n)}, G^{(n)}][G^{(n)}, N][N, G^{(n)}][N, N].\end{aligned}$$

Del lema 7.1.5 (2) se sigue que $[G^{(n)}, N] \leq N$ si y solo si $G^{(n)} \leq N_G(N)$. Dado que N es normal en G, se verifica que $N_G(N) = G$. Por tanto,

$$[G^{(n)}N, G^{(n)}N] \leq [G^{(n)}, G^{(n)}]NNN = G^{(n+1)}N.$$

En consecuencia, $(G/N)^{(n+1)} \leq G^{(n+1)}N/N$.

(3) Se sigue inmediatamente del lema 7.1.5 (3).

(4) Nuevamente procedemos por inducción sobre n. Si $n = 0$, entonces la afirmación es clara. Supongamos como hipótesis de inducción que $(G \times H)^{(n)} = G^{(n)} \times H^{(n)}$. Entonces

$$\begin{aligned}(G \times H)^{(n+1)} &= ((G \times H)^{(n)})' \\ &= (G^{(n)} \times H^{(n)})' \\ &= [G^{(n)} \times H^{(n)}, G^{(n)} \times H^{(n)}] \\ &= [G^{(n)}, G^{(n)}] \times \underbrace{[G^{(n)}, H^{(n)}]}_{=0} \times \underbrace{[H^{(n)}, G^{(n)}]}_{=0} \times [H^{(n)}, H^{(n)}] \\ &= [G^{(n)}, G^{(n)}] \times [H^{(n)}, H^{(n)}] \\ &= G^{(n+1)} \times H^{(n+1)}. \quad \square\end{aligned}$$

7.3 Grupos solubles finitos

7.3.1 Definición. G se denomina `soluble` si existe $n \in \mathbb{N}$ tal que $G^{(n)} = 1$. El número natural más pequeño n con esta propiedad se llama el `grado de solubilidad` de G.

7.3.2 Ejemplos. (1) Todo grupo abeliano es soluble.

(2) $\mathrm{Sym}(3)$ es soluble. En efecto, del ejemplo 7.1.8 se sigue que $\mathrm{Sym}(3)' = \mathrm{Alt}(3)$. Dado que $\mathrm{Alt}(3)$ es abeliano, se tiene que $\mathrm{Alt}(3)' = (1)$.

(3) $\mathrm{Sym}(4)$ es soluble. Nuevamente se tiene que

$$\begin{aligned}\mathrm{Sym}(4)' &= \mathrm{Alt}(4)\\ &= \{(1),(124),(134),(234),(132),(123),(142),(143),(243),\\ &\quad (12)(34),(13)(24),(14)(23)\}\\ \mathrm{Alt}(4)' &= \{(1),(12)(34),(13)(24),(14)(23)\} = V_4.\end{aligned}$$

Dado que V_4 es abeliano, se tiene que $V_4' = (1)$.

(4) Para todo $n \geq 5$ se verifica que $\mathrm{Sym}(n)$ no es soluble. En efecto, del ejemplo 7.1.8 se tiene que para todo $n \geq 5$ y todo $k \in \mathbb{N}$ se verifica que $\mathrm{Sym}(n)^{(k)} = \mathrm{Alt}(n)$. Por lo tanto, $\mathrm{Sym}(n)^{(k)} \neq \{(1)\}$ para todo $k \in \mathbb{N}$.

7.3.3 Teorema. Sean $N, M \trianglelefteq G$ y $U \leq G$.

(1) Si G es soluble, entonces U y G/N también lo son.

(2) Si N y G/N son solubles, entonces G es soluble.

(3) Si N y M son solubles, entonces NM es soluble.

Demostración. (1) Si G es soluble, entonces existe $n \in \mathbb{N}$ tal que $G^{(n)} = 1$. Dado que $U^{(j)} \subseteq G^{(j)}$ para todo $j \in \mathbb{N}$, se sigue entonces que U es soluble.

Por otro lado,

$$(G/N)^{(n)} = G^{(n)}N/N = N/N = 1.$$

Por lo tanto, G/N también es soluble.

(2) Supongamos que $N^{(k)} = 1$ y $(G/N)^{(m)} = \{N\}$. Entonces $G^{(m)} \subseteq N$, y se sigue que

$$G^{(m+k)} \subseteq \left(G^{(m)}\right)^{(k)} \subseteq N^{(k)} = 1,$$

lo cual demuestra que G es soluble.

(3) Del segundo teorema de isomorfía se tiene que $NM/N \cong M/(N \cap M)$. Dado que por hipótesis M es soluble, se sigue de (1) que los grupos $N \cap M$ y $M/(N \cap M)$ son solubles. Por lo tanto, NM/N es soluble.

Por hipótesis se tiene que N es soluble. Por lo cual, usando (2) se sigue que NM es soluble. □

7.3.4 Teorema. Sea G y H grupos y $N, M \trianglelefteq G$.

(1) Si G y H son solubles, entonces $G \times H$ también lo es.

(2) Si G/N y G/M son solubles, entonces $G/(N \cap M)$ es soluble. En particular, si $N \cap M = 1$, entonces G es soluble.

Demostración. (1) Supongamos que $G^{(n)} = 1$ y $H^{(m)} = 1$ y sea $k := \max\{m, n\}$. Entonces

$$(G \times H)^{(k)} = G^{(k)} \times H^{(k)} = 1.$$

(2) En el teorema 7.1.11 se demostró que $G/(N \cap M)$ es isomorfo a un subgrupo de $G/N \times G/M$. En consecuencia, $G/(N \cap M)$ es soluble. □

7.3.5 Observación. Existe una relación entre la solubilidad de un grupo y la existencia de cadenas con factores abelianos. En efecto, si G es un grupo finito soluble, entonces existe $n \in \mathbb{N}$ tal que $G^{(n)} = 1$, y además existe la cadena

$$G = G^{(0)} \trianglerighteq G^{(1)} \trianglerighteq \cdots \trianglerighteq G^{(n)} = 1.$$

Dado que G/G' es abeliano, se tiene que para la cadena anterior se verifica que cada factor $G^{(i)}/G^{(i+1)}$ es abeliano.

En el siguiente teorema demostramos que la existencia de una cadena en un grupo G con factores abelianos garantiza la solubilidad de este.

7.3.6 Teorema. Las siguientes afirmaciones son equivalentes:

(1) G es soluble.

(2) Existe una cadena de subgrupos de G

$$1 = N_0 \leq N_1 \leq \cdots \leq N_n = G,$$

con $N_j \trianglelefteq G$ y N_{j+1}/N_j abeliano para todo $j \in \{0, \ldots, n-1\}$.

(3) Existe una cadena de subgrupos de G

$$1 = N_0 \leq N_1 \leq \cdots \leq N_r = G,$$

con $N_j \trianglelefteq N_{j+1}$ y N_{j+1}/N_j abeliano para todo $j \in \{0, \ldots, r-1\}$.

Demostración. (1) $\Rightarrow$ (2). Si G es soluble de grado n, entonces la cadena

$$G = G^{(0)} \geq G^{(1)} \geq \cdots \geq G^{(n)} = 1$$

es una serie normal de G con factores abelianos.

(2) $\Rightarrow$ (3) Evidente.

(3) $\Rightarrow$ (1) Supongamos que existe una serie subnormal de G

$$1 = N_0 \leq N_1 \leq \cdots \leq N_r = G,$$

con N_{j+1}/N_j abeliano para todo $j \in \{0, \ldots, r-1\}$.

Demostramos por inducción sobre j que $G^{(j)} \leq N_{r-j}$. Si $j = 0$, entonces la afirmación es inmediata.

Como hipótesis de inducción supongamos que $G^{(j-1)} \leq N_{r-j+1}$. Entonces

$$G^{(j)} = (G^{(j-1)})' \leq (N_{r-j+1})' \leq N_{r-j}.$$

En particular $G^{(r)} \leq N_0 = 1$ y se tiene que G es soluble.

7.3.7 Teorema. Si $|G| = p^n$, con p primo y $n \in \mathbb{N}_0$, entonces G es soluble.

Demostración. Procedamos por inducción sobre $|G|$. Es claro que si $n = 0$, entonces G es soluble. Supongamos entonces que para todo grupo con orden menor que $|G|$ se cumple la afirmación. Dado que G es un p-grupo, se tiene que $Z(G) \neq 1$, por lo tanto, $|G/Z(G)| < |G|$ y así $G/Z(G)$ es soluble. Por otro lado, $Z(G)$ es soluble, ya que es abeliano. Usando el teorema 7.3.3 (2) se tiene que G es soluble. □

7.3.8 Corolario. Si $|G| = pq$, con p y q números primos, entonces G es soluble.

Demostración. Si $p = q$, entonces el resultado se tiene inmediatamente. Supongamos entonces, sin perder generalidad, que $p < q$. Del teorema 6.3.3 se sigue que G admite un único subgrupo $N \trianglelefteq G$, con $|N| = q$. Por lo tanto, N es cíclico y, en consecuencia, soluble. Dado que $|G/N| = p$, con el mismo argumento se tiene que G/N es soluble. Por lo cual, G es soluble. □

7.4 Ejercicios

1. Demuestre el lema 7.1.4.
2. Sean $g, h \in G$. Si g conmuta con $[g,h]$, demuestre que $[g,h]^n = [g^n, h]$ para todo $n \in \mathbb{N}$.
3. Sean $g_1, \ldots, g_n \in G$. Demuestre que
$$[g_1, [g_2, \ldots, g_n]^{-1}] = [g_2, \ldots, g_n]^{-1}[g_1, \ldots, g_n]^{-1}[g_2, \ldots, g_n].$$
4. Sean $U_1, \ldots U_n \trianglelefteq G$. Demuestre que
$$[U_1, \ldots U_n] = [U_1, [U_2, [\cdots [U_{n-1}, U_n] \cdots].$$
5. Sea $n \in \mathbb{N}$. Demuestre que
$$K_n(G) = \langle [g_1, \ldots, g_n] \mid g_1, \ldots, g_n \in G \rangle.$$
6. Sean $N \trianglelefteq G$ y $A, B, C \leq G$. Demuestre que si $[B,[C,A]] \leq N$ y $[C,[A,B]] \leq N$, entonces $[A,[B,C]] \leq N$.
7. Demuestre que si G es perfecto, entonces $Z(G/Z(G))$ es trivial.
8. Demuestre que para todo grupo G se verifica que G/G' es abeliano.
9. Sea G un grupo y $A, B, C \leq G$. Demuestre que
Si $B \leq N_G(A) \cap N_G(C)$, entonces $[A, BC] = [A,B][A,C]$.
10. Sea G el grupo definido por
$$G = \langle a, b \mid a^4 = 1,\ b^2 = a^2, bab^{-1} = a^{-1} \rangle.$$
¿Es G soluble?
11. Sea G un grupo, $A, B \leq G$ y $H = \langle A, B \rangle$. Demuestre que
    (a) $A[A,B]$, $B[A,B] \trianglelefteq H$.
    (b) $A[A,B]B[A,B] = H$.
12. Sea K un cuerpo y
$$G := \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in K, \quad ac \neq 0 \right\}.$$
¿Es G un grupo soluble?

13. Sea G un grupo finito. Establecer y demostrar una cadena de implicaciones para las siguientes propiedades de un grupo finito G:

    (a) G es abeliano

    (b) G es cíclico

    (c) G es soluble

14. Sea G un grupo y definamos $n := |G : Z(G)|$.

    (a) Demuestre que existen a lo mas n^2 conmutadores distintos en G.

    (b) Demuestre que $[x, y]^{n+1} = [x, y^2][yxy^{-1}, y]^{n-1}$.

15. Demuestre que un subgrupo normal N de un grupo finito G es maximal si y solo si el grupo G/N es simple.

16. Sea G un grupo cíclico de orden 12, digamos $G = \langle g \rangle$. Muestre dos series de composición, distintas, de G.

17. Demuestre que $\mathrm{Alt}(4)'$ es isomorfo a V_4.

18. Sea G un grupo finito, con $|G| = p^a q$, donde p y q son números primos y $a \in \mathbb{N}$. Demuestre que G es soluble.

19. Sea G un grupo finito, con $|G| = pqr$, donde p, q y r son números primos. Demuestre que G es soluble.

20. Sea G un p-grupo finito y sea $x, y \in G$. Demuestre que

    (a) Si $G/Z(G)$ es abeliano, entonces para todo $i \geq 2$

    $$[x, y]^i = [x^i, y] \quad \text{y} \quad (xy)^i = x^i y^i [y^{-1}, x^{-1}]^{\binom{i}{2}}.$$

    (b) Si $G/Z(G)$ es abeliano elemental, entonces $(xy)^p = x^p y^p$ para todo p impar y $(xy)^4 = x^4 y^4$ para $p = 2$.

CAPÍTULO 8

GRUPOS NILPOTENTES

La teoría de grupos finitos ha estado más bien en un estado de estancamiento en los últimos años. Esto ciertamente no se debió a la falta de problemas no resueltos. Al igual que en la teoría de los números, en la teoría de grupos, es más fácil hacer preguntas que responderlas. Si presento aquí algunas investigaciones sobre grupos finitos, es con la esperanza de despertar un nuevo interés en el campo.
(Richard Brauer - International Congress of Mathematicians - 1954)

A lo largo de este capítulo G denota siempre un grupo.

8.1 Series centrales

8.1.1 Definición. Una serie de subgrupos normales de G, digamos

$$G = U_0 \geq U_1 \geq \cdots \geq U_n = 1,$$

se denomina `central` si $U_i/U_{i+1} \leq Z(G/U_{i+1})$ para todo i.

8.1.1 Serie central descendente

8.1.2 Definición. Para $n \in \mathbb{N}$ definimos recursivamente los subgrupos $K_n(G)$ de la siguiente manera:

$$\begin{aligned} K_1(G) &:= G \\ K_{n+1}(G) &:= [K_n(G), G] \qquad n \geq 1. \end{aligned}$$

8.1.3 Lema. Sea G, H grupos. Entonces para todo $n \in \mathbb{N}$

(1) Si $U \leq G$, entonces $K_n(U) \leq K_n(G)$.

(2) Si $\alpha \in \mathrm{Hom}(G, H)$, entonces $\alpha(K_n(G)) \leq K_n(\alpha(G)) \leq K_n(H)$. En particular se tiene que $K_n(G)$ es un subgrupo de G completamente invariante.

(3) Si $\alpha \in \mathrm{Hom}(G, H)$ es un epimorfismo, entonces $\alpha(K_n(G)) = K_n(H)$.

(4) $K_n(G) \trianglelefteq G$ y, por lo tanto, $K_{n+1}(G) \leq K_n(G)$. Es decir, se tiene una cadena de subgrupos de G

$$G = K_1(G) \geq K_2(G) \geq \cdots$$

Demostración. (1) Procedemos por inducción sobre n. Si $n = 1$, entonces

$$K_1(U) = U \leq G = K_1(G).$$

Supongamos que la afirmación es válida para n. Es decir, supongamos que $K_n(U) \leq K_n(G)$. Entonces

$$K_{n+1}(U) = [K_n(U), U] \leq [K_n(G), G] = K_{n+1}(G).$$

(2) Procedemos por inducción sobre n. Si $n = 1$, entonces

$$\alpha(K_1(G)) = \alpha(G) = K_1(\alpha(G)) \leq K_1(H).$$

Como hipótesis de inducción supongamos que

$$\alpha(K_n(G)) \leq K_n(\alpha(G)) \leq K_n(H).$$

Entonces usando el lema 7.1.5 (3) y la hipótesis de inducción tenemos

$$\begin{aligned} \alpha(K_{n+1}(G)) &= \alpha([K_n(G), G]) \\ &\leq [\alpha(K_n(G)), \alpha(G)] \\ &\leq [K_n(\alpha(G)), \alpha(G)] \\ &= K_{n+1}(\alpha(G)) \\ &\leq K_{n+1}(H). \end{aligned}$$

Si en particular $G = H$ y $\alpha \in \mathrm{End}(G)$, entonces $\alpha(K_n(G)) \leq K_n(\alpha(G)) \leq K_n(G)$. Es decir, $K_n(G)$ es un subgrupo de G completamente invariante.

(3) Se deja como ejercicio.

(4) De (2) se sigue que $K_n(G) \trianglelefteq G$. Por lo tanto, $G = N_G(K_n(G))$. Del lema 7.1.5 (2) se sigue que esto es equivalente a

$$K_n(G) \geq [K_n(G), G] = K_{n+1}(G). \quad \square$$

8.1.4 Lema. Sean $H, K \trianglelefteq G$ con $K \leq H$. Entonces $[H, G] \leq K$ si y solo si $H/K \leq Z(G/K)$. En particular, $K_n(G)/K_{n+1}(G) \leq Z(G/K_{n+1}(G))$ para todo $n \in \mathbb{N}$.

Demostración. Supongamos que $H, K \trianglelefteq G$ con $K \leq H$. Entonces

$$\begin{aligned} [H, G] \leq K &\Leftrightarrow [H, G]K \leq K \\ &\Leftrightarrow [H, G]K/K \leq K/K \\ &\Leftrightarrow [H/K, G/K] = \{K\} \\ &\Leftrightarrow H/K \leq Z(G/K). \end{aligned}$$

Finalmente, dado que $K_{n+1}(G) = [K_n(G), G]$, el lado izquierdo de la equivalencia anterior se verifica y se tiene la afirmación. $\square$

8.1.5 Definición. La cadena de subgrupos de G, completamente invariantes,

$$G = K_1(G) \geq K_2(G) \geq \cdots \tag{8.1}$$

se denomina `serie central descendente` de G.

Presentamos en el siguiente resultado algunas propiedades de esta cadena.

8.1.6 Teorema. Sea G y H grupos y $n \in \mathbb{N}$. Entonces $K_n(G \times H) = K_n(G) \times K_n(H)$.

Demostración. Demostramos la afirmación por inducción sobre n. Si $n = 1$, entonces

$$K_1(G \times H) = G \times H = K_1(G) \times K_1(H).$$

Supongamos que la afirmación es válida para $n-1$. Entonces usando el lema 7.1.10 tenemos

$$\begin{aligned} K_n(G \times H) &= [G \times H, K_{n-1}(G \times H)] \\ &= [G \times H, K_{n-1}(G) \times K_{n-1}(H)] \\ &= [G, K_{n-1}(G)] \underbrace{[H, K_{n-1}(G)]}_{1} \underbrace{[G, K_{n-1}(H)]}_{1} [H, K_{n-1}(H)] \\ &= [G, K_{n-1}(G)][H, K_{n-1}(H)] \\ &= K_n(G) \times K_n(H). \quad \square \end{aligned}$$

8.1.2 Serie central ascendente

8.1.7 Definición. Para $n \in \mathbb{N}_0$ definimos recursivamente los subgrupos $Z_n(G)$ de la siguiente manera:

$$\begin{aligned} Z_0(G) &:= 1, \\ Z_1(G) &:= Z(G), \\ Z_{n+1}(G)/Z_n(G) &:= Z(G/Z_n(G)). \end{aligned}$$

Evidentemente se tiene una cadena de subgrupos de G

$$1 = Z_0(G) \leq Z_1(G) \leq \cdots$$

los cuales son característicos en G, como se demuestra en el siguiente lema. El subgrupo $Z_\infty(G)$ se define por

$$Z_\infty(G) := \bigcup_{j \in \mathbb{N}} Z_j(G)$$

y se denomina el `hipercentro de` G.

8.1.8 Ejemplos. (1) La serie central ascendente de un grupo abeliano G es trivial, ya que $Z(G) = G$.

(2) El centro del grupo de los cuaterniones $\mathbb{Q}_8$ (ver ejercicios del capítulo 1) tiene orden dos, por lo tanto, $Z_2(\mathbb{Q}_8) = \mathbb{Q}_8$.

En el siguiente lema demostramos que cada eslabón de la serie central ascendente de un grupo G es un subgrupo característico de G.

8.1.9 Lema. $Z_j(G)$ char G para todo j.

Demostración. Procedemos por inducción sobre j. Si $j = 0$, entonces el resultado es inmediato. Supongamos que la afirmación es válida para todo $0 \leq k \leq n$.

En el ejemplo 2.4.14 (1) se demostró que el centro de un grupo G es característico en G. A su vez, en el lema 2.4.12 (5) se demostró que si $U \leq V \leq G$ con U char G y V/U char G/U, entonces V char G. Con estos argumentos se tiene que $Z_{k+1}(G)/Z_k(G) = Z(G/Z_k(G))$ char $G/Z_k(G)$, y por hipótesis de inducción $Z_k(G)$ char G. Por lo tanto, $Z_{k+1}(G)$ char G. □

8.1.10 Definición. La cadena de subgrupos característicos de G

$$1 = Z_0(G) \leq Z_1(G) \leq \cdots \tag{8.2}$$

se denomina `serie central ascendente` de G. Del lema 8.1.4 se sigue además que

$$[Z_{n+1}(G), G] \leq Z_n(G).$$

Presentamos a continuación algunos resultados que relacionan las series centrales ascendente y descendente.

8.1.11 Lema. Sea $1 = U_0 \leq U_1 \leq \cdots \leq U_n = G$ una serie central de G. Entonces

(1) $U_j \leq Z_j(G)$ para todo $j \in \{0, \ldots, n\}$.

(2) $K_j(G) \leq U_{n-j+1}$ para todo $j \in \{1, \ldots, n+1\}$.

Demostración. (1) Procedemos por inducción sobre j. Si $j = 0$, entonces $U_0 = 1 = Z_0(G)$. Como hipótesis de inducción supongamos que $U_j \leq Z_j(G)$.

Sean ahora $x \in U_{j+1}$ y $g \in G$ cualesquiera. Dado que $U_{j+1}/U_j \leq Z(G/U_j)$, se verifica que $xU_j \in Z(G/U_j)$. Por lo tanto, $xU_jgU_j = gU_jxU_j$ o, equivalentemente, $xgU_j = gxU_j$. Esto trae como consecuencia que $x^{-1}g^{-1}xg \in U_j$.

Usando la hipótesis de inducción obtenemos que $x^{-1}g^{-1}xg \in Z_j(G)$. Entonces $xgZ_j(G) = gxZ_j(G)$. Es decir,

$$xZ_j(G)gZ_j(G) = gZ_j(G)xZ_j(G).$$

Esto es equivalente a afirmar que

$$xZ_j(G) \in Z(G/Z_j(G)) = Z_{j+1}(G)/Z_j(G).$$

Entonces $x \in Z_{j+1}(G)$, y se sigue que $U_{j+1} \leq Z_{j+1}(G)$.

(2) Procedemos por inducción sobre j. Si $j = 1$, entonces $K_1(G) = G = U_n$. Como hipótesis de inducción supongamos que $K_j(G) \leq U_{n-j+1}$.

Dado que $U_{n-j+1}/U_{n-j} \leq Z(G/U_{n-j})$, se sigue que $[U_{n-j+1}, G] \leq U_{n-j}$. Por lo cual, usando la hipótesis de inducción tenemos

$$K_{j+1}(G) = [K_j(G), G] \leq [U_{n-j+1}, G] \leq U_{n-j},$$

con lo cual se tiene la afirmación. □

Como consecuencia del teorema anterior se tiene inmediatamente que para ciertos grupos las cadenas centrales ascendente y descendente tienen la misma longitud. Una clase de estas grupos es la clase de los grupos nilpotentes.

8.2 Grupos nilpotentes finitos

8.2.1 Definición. Un grupo G se denomina `nilpotente` si admite una serie central

$$G = U_0 \geq U_1 \geq \cdots \geq U_n = 1.$$

La menor longitud de una serie central de G se denomina la `clase de nilpotencia` de G y se nota con $c(G)$.

Utilizando las series centrales ascendente y descendente podemos presentar en términos de estas una nueva caracterización de los grupos nilpotentes.

8.2.2 Teorema. Las siguientes afirmaciones son equivalentes:

(1) G es nilpotente.

(2) $K_{n+1}(G) = 1$ para algún $n \in \mathbb{N}$.

(3) $Z_n(G) = G$ para algún $n \in \mathbb{N}$.

Demostración. (1) $\Rightarrow$ (2). Supongamos que G es nilpotente y sea $1 = U_0 \leq U_1 \leq \cdots \leq U_n = G$ una serie central de G. Usando el lema 8.1.11 (2) tenemos que $K_{n+1}(G) \leq U_0 = 1$. Por lo tanto, $K_{n+1}(G) = 1$.

(2) $\Rightarrow$ (3). Definamos $U_0 := K_{n+1}(G) = 1$, $U_1 := K_n(G), \ldots, U_n := K_1(G) = G$. Usando el lema 8.1.11 (1) tenemos que $G = U_n \leq Z_n(G)$. En consecuencia, $Z_n(G) = G$.

(3) $\Rightarrow$ (1). Evidente. □

8.2.3 Corolario. Si G es un grupo nilpotente, entonces sus series centrales ascendente y descendente tienen la misma longitud.

Demostración. Es una consecuencia inmediata del teorema anterior. □

8.2.4 Ejemplos. (1) Si G es abeliano, entonces G es nilpotente y además de clase 1.

(2) Dado que $Z(\mathrm{Sym}(3)) = 1$, se sigue que $\mathrm{Sym}(3)$ no es nilpotente.

(3) Sea $\mathrm{SL}(2,3)$ el grupo de las matrices invertibles de tamaño 2×2 con determinante 1 y entradas en el cuerpo con tres elementos $\mathbb{F}_3$. Se verifica que $\mathrm{SL}(2,3)$ tiene 24 elementos y su centro está dado por

$$Z(\mathrm{SL}(2,3)) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \right\}.$$

El grupo cociente $\mathrm{SL}(2,3)/Z(\mathrm{SL}(2,3))$ es $\mathrm{PSL}(2,3)$, el grupo lineal especial proyectivo de grado dos sobre $\mathbb{F}_3$, el cual es isomorfo al grupo alternante $\mathrm{Alt}(4)$. En consecuencia,

$$Z(\mathrm{SL}(2,3)/Z(\mathrm{SL}(2,3))) \cong Z(\mathrm{Alt}(4)) = 1.$$

Por lo tanto, $Z_2(\mathrm{SL}(2,3)) = Z(\mathrm{SL}(2,3))$, y se tiene que $\mathrm{SL}(2,3)$ no es nilpotente.

8.2.5 Teorema. Sea G y H grupos, $U \leq G$ y $N, M \trianglelefteq G$. Entonces

(1) Si G es nilpotente, entonces U y G/N son nilpotentes. Además $c(U)$, $c(G/N) \leq c(G)$.

(2) Si G y H son grupos nilpotentes, entonces $G \times H$ es nilpotente de clase $m := \max\{c(G), c(H)\}$.

(3) Si $G_1, \ldots, G_k$ son grupos nilpotentes, entonces $G_1 \times \cdots \times G_k$ es nilpotente de clase $m := \max\{c(G_1), \ldots, c(G_k)\}$.

(4) Si G/N y G/M son nilpotentes, entonces $G/(N \cap M)$ es nilpotente de clase $m = \max\{c(G/N), c(G/M)\}$.

En particular, si $M \cap N = 1$, entonces G es nilpotente.

Demostración. (1) Supongamos que $K_{c+1}(G) = 1$. Dado que $U \leq G$, se sigue que $K_{c+1}(U) \leq K_{c+1}(G) = 1$. Por lo tanto, $K_{c+1}(U) = 1$.

Usando el lema 7.1.5 (3), con π el epimorfismo canónico se tiene

$$\begin{aligned}\pi([G, K_c(G)]) &= [\pi(G), \pi(K_c(G))] \\ &= [G/N, K_c(G)N/N] \\ &= [G/N, K_c(G/N)] \\ &= K_{c+1}(G/N).\end{aligned}$$

Por otro lado,

$$\begin{aligned}\pi([G, K_c(G)]) &= [G, K_c(G)]N/N \\ &= K_{c+1}(G)N/N \\ &= N/N \\ &= 1.\end{aligned}$$

Es decir, $K_{c+1}(G/N) = 1$.

(2) Del teorema 8.1.6 se sigue que

$$K_{m+1}(G \times H) = K_{m+1}(G) \times K_{m+1}(H) = 1.$$

Dado que $K_m(G) \neq 1$ o $K_m(H) \neq 1$, se tiene que $K_m(G_1 \times G_2) \neq 1$. Por lo tanto, $G_1 \times G_2$ es nilpotente de clase m.

(3) Se sigue de (2) usando inducción.

(4) Del teorema 7.1.11 se tiene que

$$G/(M \cap N) \cong \varphi(G) \leq G/M \times G/N.$$

De (1) y (2) se sigue que $G/(M \cap N)$ es nilpotente de clase $c \leq \max\{c(G/N), c(G/M)\}$.

Por otro lado, del tercer teorema de isomorfía tenemos que

$$G/(M \cap N)/M/(M \cap N) \cong G/M \quad \text{y} \quad G/(M \cap N)/N/(M \cap N) \cong G/N.$$

Entonces de (1) se sigue que $c \geq \max\{c(G/N), c(G/M)\}$ y se tiene la igualdad. □

8.2.6 Observación. A diferencia de los grupos solubles, si G es un grupo y $N \trianglelefteq G$, la nilpotencia de G/N y de N no garantiza la nilpotencia de G. En efecto, si $G = \mathrm{Sym}(3)$ y $N = \mathrm{Alt}(3)$, entonces se tiene que G/N y N son nilpotentes, pero G no lo es.

8.2.7 Lema. Si G es un p-grupo finito, entonces G es nilpotente.

Demostración. Usamos inducción matemática sobre $|G|$. Si $|G| = 1$, claramente G es nilpotente. Como hipótesis de inducción supongamos que la afirmación es válida para todo grupo cuyo orden sea menor que $|G|$.

Si $|G| > 1$, entonces $Z(G) \neq 1$ y el grupo cociente $G/Z(G)$ tiene orden menor que $|G|$. usando la hipótesis de inducción tenemos que $G/Z(G)$ es nilpotente. Es decir, existe $c \in \mathbb{N}$ tal que $K_{c+1}(G/Z(G)) = 1$. Sea $\pi : G \longrightarrow G/Z(G)$ el epimorfismo canónico. Entonces

$$\pi(K_{c+1}(G)) = K_{c+1}(\pi(G)) = K_{c+1}(G/Z(G)) = 1.$$

En consecuencia, $K_{c+1}(G) \leq \ker(\pi) = Z(G)$. Por lo tanto,

$$K_{c+2}(G) = [K_{c+1}(G), G] \leq [Z(G), G] = 1.$$

Esto demuestra que G es nilpotente. □

8.2.8 Observación. Una consecuencia del teorema anterior es que un grupo finito G es nilpotente de clase c si y solo si $G/Z(G)$ es nilpotente de clase $c - 1$.

8.2.9 Teorema. Sea G nilpotente y $1 \neq N \trianglelefteq G$. Entonces $N \cap Z(G) \neq 1$. En particular, el centro de un grupo nilpotente es no trivial.

DEMOSTRACIÓN. Supongamos que $Z_n(G) = G$. Entonces considerando la serie central ascendente tenemos que existe $j \in \{1, \ldots, n-1\}$ tal que $N \cap Z_j(G) = 1$, pero $N \cap Z_{j+1}(G) \neq 1$. Entonces

$$[G, N \cap Z_{j+1}(G)] \leq [G, N] \cap [G, Z_{j+1}(G)].$$

La normalidad de N implica que $[G, N] \leq N$, y además para la serie central ascendente se verifica que $[G, Z_{j+1}(G)] \leq Z_j(G)$. Por lo tanto,

$$[G, N \cap Z_{j+1}(G)] \leq N \cap Z_j(G) = 1.$$

Esto demuestra que $N \cap Z_{j+1}(G) \leq Z(G)$, y claramente esto implica que $N \cap Z(G) \neq 1$. □

En los siguientes teoremas presentamos algunas caracterizaciones de los grupos nilpotentes.

8.2.10 Teorema. Si G es finito, entonces las siguientes afirmaciones son equivalentes:

(1) G es nilpotente.

(2) Si $U < G$, entonces $U < N_G(U)$.

(3) Todo subgrupo maximal de G es normal en G.

(4) Si $P \in \mathrm{Syl}_p(G)$, entonces $P \trianglelefteq G$.

(5) G es el producto directo de sus p-subgrupos de Sylow.

DEMOSTRACIÓN. (1) $\Rightarrow$ (2). Dado que $Z_0(G) = 1$ y $Z_n(G) = G$, existe $j \in \{0, \ldots, n-1\}$ tal que $Z_j(G) \leq U$, pero $Z_{j+1}(G) \nleq U$. Entonces

$$[U, Z_{j+1}(G)] \leq [G, Z_{j+1}(G)] \leq Z_j(G) \leq U.$$

Del lema 7.1.5 (2) se sigue que $Z_{j+1}(G) \leq N_G(U)$, con lo cual se tiene que $U < N_G(U)$.

(2) $\Rightarrow$ (3). Sea $M \lhd G$. Entonces $M < G$ y se tiene por hipótesis que $M < N_G(M)$. En consecuencia, $N_G(M) = G$. Es decir, M es normal en G.

(3) $\Rightarrow$ (4). Sea $P \in \mathrm{Syl}_p(G)$ con $N_G(P) < G$. Sea $M \lhd G$ tal que $N_G(P) \leq M$. Entonces del corolario 6.2.13 (2) se tiene que $M = N_G(M) = G$, lo cual es una contradicción. Entonces $N_G(P) = G$ y se tiene que $P \trianglelefteq G$.

(4) $\Rightarrow$ (5). Por hipótesis se tiene que cada p-subgrupos de Sylow de G es normal en G. Sea $|G| = p_1^{a_1} \cdots p_r^{a_r}$, con $p_i \neq p_j$ para $i \neq j$. Entonces la normalidad de cada $P_j \in \mathrm{Syl}_{p_j}(G)$ implica la unicidad de cada P_j, y dado que

$$P_j \cap \langle P_i \mid i \neq j \rangle = 1,$$

se sigue que $G = P_1 \times \cdots \times P_r$.

(5) $\Rightarrow$ (1). Dado que todo p-grupo es nilpotente, la nilpotencia de G se sigue del teorema 8.2.5 (4). $\square$

8.2.11 Definición. Sea $U \leq G$. Decimos que U es `subnormal` en G, notado $U \trianglelefteq\trianglelefteq\ G$, si existe una cadena

$$U = U_0 \leq U_1 \leq \cdots \leq U_n = G,$$

con $U_j \trianglelefteq U_{j+1}$ para todo $j \in \{0, \ldots, n-1\}$.

8.2.12 Teorema. Si G es finito, entonces las siguientes afirmaciones son equivalentes:

(1) G es nilpotente.

(2) Todo subrupo de G es subnormal.

Demostración. (1) $\Rightarrow$ (2). Sea $U \leq G$. Definamos $U_0 := U$, y además definamos inductivamente $U_j := N_G(U_{j-1})$. Dado que G es nilpotente, si $U_{j-1} \neq G$, entonces

$$|U_{j-1}| < |U_j|.$$

Como G es finito, existe $n \in \mathbb{N}$ tal que $U_n = G$ y se tiene así que U es subnormal.

(2) $\Rightarrow$ (1). Sea $P \in \mathrm{Syl}_p(G)$ y supongamos que $N_G(P) < G$. Entonces existe $U \lneq G$ tal que $N_G(P) \leq U$. Del corolario 6.2.13 (1) se sigue que $N_G(U) = U$. Por otro lado, al ser U maximal en G y subnormal, se tiene inmediatamente que $U \trianglelefteq G$. Es decir, $N_G(U) = G$, lo cual es una contradicción.

Hemos demostrado entonces que todo p-subgrupo de Sylow de G es normal en G y usamos el teorema anterior para asegurar la nilpotencia de G es nilpotente. $\square$

Como consecuencia de los teoremas anteriores tenemos el siguiente resumen que caracteriza a los grupos nilpotentes finitos.

8.2.13 Observación. Si G es finito, entonces las siguientes afirmaciones son equivalentes:

(1) G es nilpotente.

(2) Si $U < G$, entonces $U < N_G(U)$.

(3) Todo subgrupo maximal de G es normal en G.

(4) Si $P \in \mathrm{Syl}_p(G)$, entonces $P \trianglelefteq G$.

(5) G es el producto directo de sus p-subgrupos de Sylow.

(6) Todo subgrupo de G es subnormal.

8.3 Nilpotencia implica solubilidad

Hasta ahora no se ha establecido relaciones entre la nilpotencia y la solubilidad de un grupo. Demostramos al final de esta sección que todo grupo nilpotente finito es soluble y que existen grupos finitos solubles que no son nilpotentes.

Inicialmente es necesario introducir los conmutadores generalizados.

8.3.1 Definición. Sean $g_1, \ldots, g_n \in G$ y $U_1, \ldots, U_n \leq G$. Entonces

(1) $[g_1, g_2, g_3] := [[g_1, g_2], g_3]]$.

(2) Para $n > 3$ definimos

$$[g_1, g_2, \ldots, g_n] := [[g_1, g_2, \ldots, g_{n-1}], g_n]].$$

(3) $[U_1, \ldots, U_n] := \langle [g_1, \ldots, g_n] \mid g_j \in U_j, j = 1, \ldots, n \rangle$.

8.3.2 Lema. (Identidad de Hall-Witt) Sean $a, b, c \in G$. Entonces

$$[a, b^{-1}, c]^b \; [b, c^{-1}, a]^c \; [c, a^{-1}, b]^a = 1.$$

Demostración. Se deja como ejercicio. □

8.3.3 Lema. (Los tres subgrupos) Sean $A, B, C \leq G$ y $N \trianglelefteq G$. Entonces

(1) Si $[B, C, A] = 1$ y $[C, A, B] = 1$, entonces $[A, B, C] = 1$.

(2) Si $[B, C, A] \leq N$ y $[C, A, B] \leq N$, entonces $[A, B, C] \leq N$.

Demostración. (1) Sean $a \in A$, $b \in B$ y $c \in C$. Entonces $[b, c^{-1}, a] = 1$ y $[c, a^{-1}, b] = 1$. Usando usando la identidad de Hall-Witt se tiene que $[a, b^{-1}, c]^b = 1$, y por lo tanto, $[a, b^{-1}, c] = 1$. En consecuencia, $[a, b^{-1}] \in C_G(C)$ para todo $a \in A$ y $b \in B$. Dado que estos conmutadores generan a $[A, B]$, se tiene que $[A, B] \subseteq C_G(C)$. Por lo tanto, $[A, B, C] = 1$.

(2) De la identidad de Hall-Witt se sigue que

$$[a, b^{-1}, c]^b = ([c, a^{-1}, b]^{-1})^a \; ([b, c^{-1}, a]^{-1})^c \in N^a N^c = N.$$

Entonces $[a, b^{-1}, c] \in N$ para todo $a \in A$, $b \in B$ y $c \in C$. Por lo cual, $[A, B, C] \leq N$. □

8.3.4 Observación. Otra alternativa para demostrar (2) en el lema anterior es usar (1) en el grupo cociente G/N. Para ello tenga en cuenta que el uno en G/N es N.

8.3.5 Lema. Sean $m, n \in \mathbb{N}$. Entonces $[K_m(G), K_n(G)] \leq K_{m+n}(G)$.

Demostración. Procedemos por inducción sobre n. Si $n = 1$, entonces

$$[K_m(G), K_1(G)] = [K_m(G), G] = K_{m+1}(G).$$

Sea $n \geq 2$ y supongamos que la afirmación es válida para $n-1$. Entonces

$$\begin{aligned}[G, K_m(G), K_{n-1}(G)] &= [[G, K_m(G)], K_{n-1}(G)] \\ &= [K_{m+1}(G), K_{n-1}(G)] \\ &\leq K_{m+n}(G),\end{aligned}$$

además

$$\begin{aligned}[K_m(G), K_{n-1}(G), G] &= [[K_m(G), K_{n-1}(G)], G] \\ &\leq [K_{m+n-1}(G), G] \\ &= K_{m+n}(G).\end{aligned}$$

Del lema de los tres subgrupos (2) se sigue que

$$\begin{aligned}[K_m(G), K_n(G)] &= [K_n(G), K_m(G)] \\ &= [K_{n-1}(G), G, K_m(G)] \\ &\leq K_{m+n}(G). \qquad \square\end{aligned}$$

8.3.6 Lema. Para todo grupo G y todo $n \in \mathbb{N}_0$ se verifica que $G^{(n)} \leq K_{2^n}(G)$.

Demostración. Demostramos la afirmación por inducción sobre n. Si $n = 0$, entonces

$$G^{(0)} = G = K_1(G) = K_{2^0}(G).$$

Supongamos que para $n-1$ la afirmación está demostrada. Entonces aplicando el lema 8.3.5 tenemos:

$$\begin{aligned}G^{(n)} &= [G^{(n-1)}, G^{(n-1)}] \\ &\leq [K_{2^{n-1}}(G), K_{2^{n-1}}(G)] \\ &\leq K_{2^n}(G),\end{aligned}$$

con lo cual se tiene la afirmación. $\square$

8.3.7 Corolario. Todo grupo finito nilpotente es soluble.

DEMOSTRACIÓN. Sea G nilpotente y n el menor número natural con $K_{2^n}(G) = 1$. Entonces $G^{(n)} \leq K_{2^n}(G) = 1$ y se tiene que G es soluble. □

8.3.8 Observación. El recíproco de esta afirmación es en general falso. El grupo Sym(3) es soluble pero no es nilpotente. Es decir, la clase de los grupos nilpotentes finitos está contenida propiamente en la clase de los grupos finitos solubles.

8.3.9 Corolario. Si G es un grupo con longitud de derivado d y nilpotente de clases c, entonces $d < \log_2(c+1) + 1$.

DEMOSTRACIÓN. Del lema 8.3.6 se tiene que $G^{(n)} \leq K_{2^n}(G)$ para todo $n \in \mathbb{N}_0$. Dado que $1 \neq G^{(d-1)} \leq K_{2^{d-1}}(G)$ y $K_{c+1}(G) = 1$, se sigue que $c + 1 > 2^{d-1}$ y se tiene que la afirmación. □

8.3.10 Corolario. Si G es nilpotente de clases $c \leq 3$, entonces G' es abeliano.

DEMOSTRACIÓN. Del corolario anterior se sigue que la longitud de derivado $d < 3$. Por lo tanto, $G'' = 1$, y así G' es abeliano. □

8.3.11 Teorema. Sea G un p-grupo. Si $M \lessdot G$, entonces $M \trianglelefteq G$ y además $|G : M| = p$.

DEMOSTRACIÓN. Dado que todo p-grupo es nilpotente, se sigue que $M \triangleleft G$. La maximalidad de M implica que G/M no admite subgrupos no triviales. Por lo tanto, del teorema de Cauchy se sigue que $|G/M| = p$ y se tiene el resultado. □

8.4 Ejercicios

1. Sean $g_1, \ldots, g_n \in G$. Demuestre que

$$[[g_1, \ldots, g_n]^{-1}, g_{n+1}] = ([g_1, \ldots, g_{n+1}]^{[g_1,\ldots,g_n]^{-1}})^{-1}.$$

2. Sean $k \in \mathbb{N}$ y $N_1, \ldots, N_k \trianglelefteq G$. Entonces

$$[N_1, \ldots, N_k] = [\ldots[[N_1, N_2], N_3]\ldots, N_k]. \tag{8.3}$$

3. Sean $U_1, \ldots U_n \trianglelefteq G$. Demuestre que

$$[U_1, \ldots U_n] = [U_1, [U_2, [\cdots[U_{n-1}, U_n]\cdots].$$

4. Sea $n \in \mathbb{N}$. Demuestre que $K_n(G) = \langle [g_1, \ldots, g_n] \mid g_1, \ldots, g_n \in G \rangle$. Es decir,
$$K_n(G) = [\underbrace{G, \ldots, G}_{n-\text{veces}}].$$

5. Demuestre que $K_n(G/K_n(G)) = 1$.

6. Sean $N \trianglelefteq G$ y $A, B, C \leq G$. Demuestre que si $[B,[C,A]] \leq N$ y $[C,[A,B]] \leq N$, entonces $[A,[B,C]] \leq N$.

7. Demuestre que si G es perfecto, entonces $Z(G/Z(G))$ es trivial.

8. Sea G un grupo nilpotente y $1 \neq N \trianglelefteq G$. Demuestre que $N \cap Z(G) \neq 1$.

9. Sea G y H grupos y $m, n \in \mathbb{N}$. Demuestre que
   (a) $K_m(K_n(G)) \leq K_{mn}(G)$
   (b) $[K_m(G), Z_n(G)] \leq Z_{n-1}(G)$ si $n \geq m$.

10. Demuestre la identidad de Hall - Witt (Lema 8.3.2).

11. Demuestre que para todo grupo G se verifica que G/G' es abeliano.

12. Sea G un grupo y $A, B, C \leq G$. Demuestre que
    Si $B \leq N_G(A) \cap N_G(C)$, entonces $[A, BC] = [A, B][A, C]$.

13. Demuestre que todo grupo abeliano que admita una serie de composición es finito.

14. Sea G el grupo definido por
$$G = \langle a, b \mid a^4 = 1,\ b^2 = a^2, bab^{-1} = a^{-1} \rangle.$$
    Determine G'. ¿Es G soluble?

15. Sea G un grupo, $A, B \leq G$ y $H = \langle A, B \rangle$. Demuestre que
    (a) $A[A,B]$, $B[A,B] \trianglelefteq H$.
    (b) $A[A,B]B[A,B] = H$.

16. Sea G un grupo nilpotente de orden n y $m \mid n$. Demuestre que G admite un subgrupo de orden m. ¿Qué puede decirse de la afirmación anterior si G es soluble?

17. Sea K un cuerpo y
$$G := \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in K, \quad ac \neq 0 \right\}$$
    Determine la serie central ascendente de G. ¿Es G un grupo nilpotente? ¿Es soluble?

18. Sea G un grupo finito. Establecer y demostrar una cadena de implicaciones para las siguientes propiedades de un grupo finito G:

    (a) G es nilpotente.

    (b) G es abeliano.

    (c) G es cíclico.

    (d) G es soluble.

19. Sea G un grupo y definamos $n := |G : Z(G)|$.

    (a) Demuestre que existen a lo mas n^2 conmutadores distintos en G.

    (b) Demuestre que $[x, y]^{n+1} = [x, y^2][yxy^{-1}, y]^{n-1}$.

20. Halle la serie central ascendente y descendente de $G := \mathrm{Sym}(3)$. ¿Es G soluble? ¿Es nilpotente?

21. Encuentre refinamientos equivalentes de las siguientes cadenas del grupo aditivo $\mathbb{Z}$:

    (a) $\{0\} \leq 30\mathbb{Z} \leq 10\mathbb{Z} \leq 2\mathbb{Z} \leq \mathbb{Z}$.

    (b) $\{0\} \leq 24\mathbb{Z} \leq 3\mathbb{Z} \leq \mathbb{Z}$.

22. Demuestre que todo grupo finito admite una serie de composición.

23. Demuestre que un subgrupo normal N de un grupo finito G es maximal si y solo si el grupo G/N es simple .

24. Sea G un grupo cíclico de orden 12, digamos $G = \langle g \rangle$. Muestre dos series de composición, distintas, de G.

25. Demuestre que $Alt(4)'$ es isomorfo a V_4.

26. Demuestre que si G es un grupo perfecto, entonces $Z(G/Z(G))$ es trivial.

27. Sea G un grupo nilpotente finito, $x, y \in G$ con $\mathrm{mcd}(\mathrm{ord}(x), \mathrm{ord}(y)) = 1$. Demuestre que $xy = yx$.

28. Sea G un grupo finito y $N \leq Z(G)$. Demuestre que si G/N es nilpotente, entonces G también lo es.

29. Sea G un grupo finito, con $|G| = p^a q$, donde p y q son números primos y $a \in \mathbb{N}$. Demuestre que G es soluble.

30. Sea G un grupo finito, con $|G| = pqr$, donde p, q y r son números primos. Demuestre que G es soluble.

31. Sea G un p-grupo finito y sea $x, y \in G$.

32. Sea G un grupo finito. Demuestre que las siguientes afirmaciones son equivalentes:

    (a) G es soluble.

    (b) Todo factor de composición de G tiene orden un número primo

    (c) Todo factor principal de G es un p-grupo abeliano elemental para algún número primo p.

33. Sea G un grupo finito. Demuestre que las siguientes afirmaciones son equivalentes:

    (a) G es nilpotente.

    (b) Todo factor principal de G es central.

34. Sea $G \neq 1$ un grupo finito soluble y q un número primo y suponga que $O_q(G) \neq 1$. Sea $N := O_q(G)$ y $|N| = q^n$. Suponga además que G admite un subgrupo maximal M con $\mathtt{Core}_G(M) = 1$. Demuestre que

    (a) N es un abeliano elemental.

    (b) M es un complemento de N en G. En particular se tiene que $|G : M| = q^n$.

    (c) N es un subgrupo normal minimal de G.

    (d) $C_G(N) = N$. Por lo tanto, N es el único subgrupo normal minimal de G.

    Suponga adicionalmente que existe un número primo p tal que $O_p(M) \neq 1$. Entonces para tal primo p se verifica que

    (a) $q^n \equiv 1 \bmod p$; en particular $p \neq q$ y

    (b) Todo complemento de N en G es conjugado con M.

35. Sea G un grupo finito y N un subgrupo normal minimal de G, el cual es además un p-grupo abeliano elemental. Demuestre que $|N| = p$ si y solo si $G/C_G(N)$ es abeliano y su exponente divide a $p - 1$.

CAPÍTULO 9

EL TEOREMA DE JORDAN-HÖLDER

... hasta principios de la década de los 60, realmente no se conocía nada de interés real sobre los grupos simples finitos.
(Richard Brauer - International Congress of Mathematicians - 1970)

9.1 El lema de Zassenhaus

9.1.1 Definición. Sea $\mathcal{C} = \{U_0, U_1, \ldots, U_n\}$, con respecto a la inclusión, una cadena de subgrupos de G.

(1) Decimos que $\mathcal{C}$ es una `serie` de G si se verifica que

$$1 = U_0 \subseteq U_1 \subseteq \cdots \subseteq U_n = G.$$

(2) $\mathcal{C}$ se llama una serie `subnormal` de G si para todo $i \in \{1, \ldots, n-1\}$ se verifica que

$$U_i \trianglelefteq U_{i+1}.$$

Si además $U_i \trianglelefteq G$ para todo $i \in \{1, \ldots, n-1\}$, entonces decimos que $\mathcal{C}$ es una serie `normal` de G. Los grupos cocientes U_{i+1}/U_i se denominan `factores` de la serie subnormal y el número natural n se denomina `longitud` de $\mathcal{C}$. Si $U_i \neq U_{i+1}$ para todo $i \in \{0, \ldots, n-1\}$, entonces decimos que $\mathcal{C}$ es una serie `sin repeticiones`.

(3) Sea $\mathcal{C}' = \{V_0, V_1, \ldots, V_m\}$ una serie subnormal de G. Decimos que $\mathcal{C}'$ es un `refinamiento` de $\mathcal{C}$ si existe una función inyectiva

$$\pi : \{1, \ldots, n\} \longrightarrow \{1, \ldots, m\}$$

tal que $U_i = V_{\pi(i)}$ para todo $i \in \{1, \ldots, n\}$. Si $m > n$, entonces el refinamiento se denomina `propio`.

(4) Las serie subnormales $\mathcal{C} = \{U_0, U_1, \ldots, U_n\}$ y $\mathcal{C}' = \{V_0, V_1, \ldots, V_m\}$ se denominan `equivalentes` o `isomorfas` si $m = n$ y existe una permutación $\pi \in \mathrm{Sym}(m)$ tal que para todo $i \in \{1, \ldots, m\}$ se verifica que $U_{i+1}/U_i \cong V_{\pi(i)+1}/V_{\pi(i)}$.

9.1.2 Ejemplos. (1) G posee la serie normal $1 \trianglelefteq G$, cuyo único factor es $G/1 \cong G$.

(2) Sea $G = \mathrm{Sym}(4)$. Consideremos las cadenas $\mathcal{C}$ y $\mathcal{C}'$ dadas, respectivamente, por

$$(1) \trianglelefteq \langle (12)(34) \rangle \trianglelefteq \langle (12)(34), (13)(24) \rangle \trianglelefteq \mathrm{Alt}(4) \trianglelefteq G$$
$$(1) \trianglelefteq \langle (12)(34), (13)(24) \rangle \trianglelefteq G.$$

Se verifica que $\mathcal{C}$ es una serie subnormal de G, pero no es normal. $\mathcal{C}'$ es una serie normal de G. Además $\mathcal{C}$ es un refinamiento propio de $\mathcal{C}'$.

(3) Sea $G = \mathbb{Z}$. Entonces la cadena $\{0\} \trianglelefteq 8\mathbb{Z} \trianglelefteq 4\mathbb{Z} \trianglelefteq 2\mathbb{Z} \trianglelefteq \mathbb{Z}$ es una cadena normal de G.

(4) Sea $G = \mathbb{Z}/6\mathbb{Z}$. Entonces las series normales $\{0\} \trianglelefteq 2\mathbb{Z}/6\mathbb{Z} \trianglelefteq G$ y $\{0\} \trianglelefteq 3\mathbb{Z}/6\mathbb{Z} \trianglelefteq G$ son equivalentes o isomorfas.

(5) Si $G = \langle g \rangle$ tiene orden 24, entonces las series normales $1 \trianglelefteq \langle g^4 \rangle \trianglelefteq \langle g^2 \rangle \trianglelefteq G$ y $1 \trianglelefteq \langle g^{12} \rangle \trianglelefteq \langle g^6 \rangle \trianglelefteq G$ son equivalentes o isomorfas.

El siguiente resultado es conocido como el lema de la mariposa o el lema de Zassenhaus[1]. Este resultado nos permite obtener una técnica para refinar series normales o series subnormales.

9.1.3 Lema. (Zassenhaus, 1934) Sean $U, V \leq G$, $U_0 \trianglelefteq U$, $V_0 \trianglelefteq V$. Entonces

(1) $(U_0 \cap V)(U \cap V_0) \trianglelefteq (U \cap V)$

(2) $U_0(U \cap V_0) \trianglelefteq U_0(U \cap V)$

[1]Hans Julius Zassenhaus (Koblenz, 1912-Columbus, 1991), matemático judío-alemán. Zassenhaus hizo su doctorado bajo la dirección de E. Artin en Hamburgo. Trabajó en en teoría de grupos, cristalografía, teoría de órdenes, teoría de representaciones, teoría algebraica de números, geometría, álgebras de Lie, didáctica e historia de las matemática.

(3) $V_0(V \cap U_0) \trianglelefteq V_0(U \cap V)$

(4) $U_0(U \cap V)/U_0(U \cap V_0) \cong (U \cap V)/(U_0 \cap V)(U \cap V_0) \cong V_0(U \cap V)/V_0(V \cap U_0)$.

En el siguiente diagrama se resaltan las relaciones de contenencia entre los subgrupos mencionados en el lema de Zassenhaus. Como es usual, si dos subgrupos en el diagrama están unidos por un segmento, se entiende que el ubicado en la posición inferior es un subgrupo del otro.

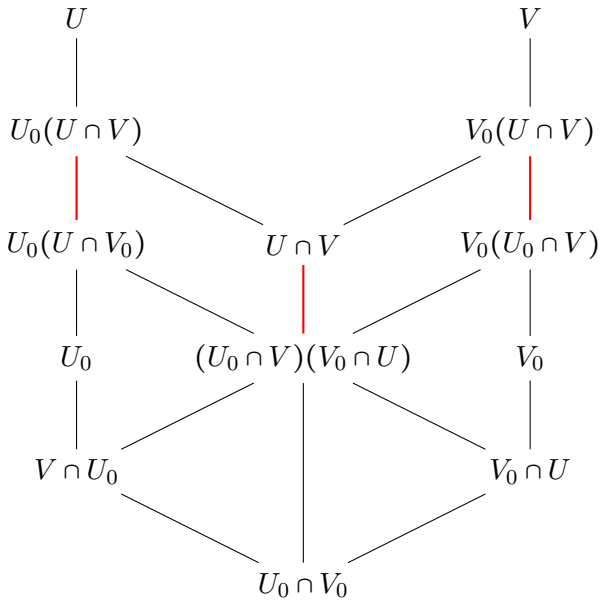


Figura 9.1: Lema de Zassenhaus

Demostración. Demostremos inicialmente que cada uno de los productos que aparecen en las afirmaciones del lema son efectivamente grupos.

(a) Dado que $U_0 \trianglelefteq U$ y $(U \cap V) \leq U$, del teorema 1.2.24 se verifica que $U_0(U \cap V) = (U \cap V)U_0$. Por lo tanto, $U_0(U \cap V) \leq U$.

(b) Dado que $V_0 \trianglelefteq V$ y $(U \cap V) \leq V$, usando nuevamente del teorema 1.2.24 se verifica que $V_0(U \cap V) = (U \cap V)V_0$. Por lo cual, $V_0(U \cap V) \leq V$.

(c) Dado que $U_0 \trianglelefteq U$ y $(U \cap V_0) \leq U$, se tiene también que $U_0(U \cap V_0) \leq U$. De manera similar se tiene que $V_0(V \cap U_0) \leq V$.

(d) Dado que $V_0 \trianglelefteq V$ y $(U \cap V) \leq V$, del lema 2.1.9 (1) se sigue que $U \cap V_0 = (U \cap V) \cap V_0 \trianglelefteq U \cap V$. De manera similar se demuestra que $U_0 \cap V \trianglelefteq U \cap V$.

Demostramos ahora las afirmaciones del lema:

(1) De (4) se tiene que $U \cap V_0 \trianglelefteq U \cap V$ y $U_0 \cap V \trianglelefteq U \cap V$. Usando el lema 2.1.9 (3) se tiene que $(U_0 \cap V)(U \cap V_0) \trianglelefteq (U \cap V)$.

(2) Consideremos la función $\pi : U_0(U \cap V) \longrightarrow (U \cap V)/(U_0 \cap V)(U \cap V_0)$ definida por

$$\pi(xy) = y(U_0 \cap V)(U \cap V_0), \quad x \in U_0,\ y \in U \cap V.$$

Definamos $N := (U_0 \cap V)(U \cap V_0)$.

Demostramos π está bien definida. Sean $x_1, x_2 \in U_0$ y $y_1, y_2 \in U \cap V$ con $x_1 y_1 = x_2 y_2$. Entonces

$$y_1 y_2^{-1} = x_1^{-1} x_2 \in U_0 \cap (U \cap V) = U_0 \cap V \subseteq N.$$

Por lo tanto, $y_1 N = y_2 N$. Entonces $\pi(x_1 y_1) = \pi(x_2 y_2)$.

Demostramos π es un homomorfismo. Dado que $U_0 \trianglelefteq U$ para todo $y_1 \in U \cap V$ se verifica que $y_1 U_0 = U_0 y_1$. En consecuencia,

$$\begin{aligned}
\pi(x_1 y_1 x_2 y_2) &= \pi(x_1 x_3 y_1 y_2) \text{para algún } x_3 \in U_0 \\
&= y_1 y_2 N \\
&= y_1 N y_2 N \\
&= \pi(x_1 y_1)\pi(x_2 y_2).
\end{aligned}$$

Demostramos π es un epimorfismo. Es claro que dado $xN \in (U \cap V)/N$, existe $xy \in U_0(U \cap V)$ tal que $\pi(xy) = yN$.

Determinamos el núcleo de π. Sean $x_1 \in U_0$ y $y_1 \in U \cap V$. Entonces

$$\begin{aligned}
x_1 y_1 \in \ker(\pi) &\Leftrightarrow \pi(x_1 y_1) = N. \\
&\Leftrightarrow y_1 N = N \\
&\Leftrightarrow y_1 \in N \\
&\Leftrightarrow x_1 y_1 \in U_0 N \\
&\Leftrightarrow x_1 y_1 \in U_0(U_0 \cap V)(U \cap V_0).
\end{aligned}$$

Dado que $U_0(U_0 \cap V) = U_0$, se tiene que $U_0(U_0 \cap V)(U \cap V_0) = U_0(U \cap V_0)$, y de allí

$$x_1 y_1 \in \ker(\pi) \Leftrightarrow x_1 y_1 \in U_0(U \cap V_0).$$

Por lo tanto, $\ker(\pi) = U_0(U \cap V_0)$. Entonces $U_0(U \cap V_0) \trianglelefteq U_0(U \cap V)$.

(3) Aplicando el primer teorema de isomorfía tenemos

$$U_0(U \cap V)/U_0(U \cap V_0) \cong (U \cap V)/(U_0 \cap V)(U \cap V_0).$$

(4) Se deja como ejercicio. □

9.2 El teorema de Schreier

El siguiente resultado es conocido como el teorema de refinamiento de Schreier[2]. En 1928 Otto Schreier encontró un refinamiento importante del teorema de Jordan-Hölder, exactamente 39 años después de la publicación del trabajo de Hölder. No deja de sorprender el hecho que un teorema tan extendido y básico pueda ser profundizado después de tanto tiempo. Mas sorprendente aún es que esto sucedió nuevamente; Hans Zassenhaus en 1934 descubrió una segunda mejora de la demostración, que es la que se presentó anteriormente.

9.2.1 Teorema. (Schreier, 1928) Cualquier par de cadenas o series subnormales de G admiten refinamientos equivalentes o isomorfos.

Demostración. Sean $\mathcal{C}_1$ y $\mathcal{C}_2$ series subnormales de G dadas, respectivamente, por

$$1 = U_0 \subseteq U_1 \subseteq \cdots \subseteq U_n = G$$

y

$$1 = V_0 \subseteq V_1 \subseteq \cdots \subseteq V_m = G.$$

Para cada $i \in \{0, 1, \ldots, n-1\}$ introducimos entre los grupos U_i y U_{i+1} una cadena de subgrupos, no necesariamente diferentes, de la siguiente manera:

$$U_{i,j} := U_i(U_{i+1} \cap V_j), \quad j \in \{0, 1, \ldots, m\}.$$

Note que para todo $i \in \{0, 1, \ldots, n-1\}$

$$U_i = U_{i,0} \leq U_{i,1} \leq \cdots \leq U_{i,m-1} \leq U_{i,m} = U_{i+1}.$$

Se verifica además que

$$U_{i,m} = U_{i+1} = U_{i+1,0}.$$

Usando el lema de Zassenhaus podemos afirmar que de esta forma se obtiene una nueva serie subnormal de G, digamos $\mathcal{C}_1'$, la cual es un refinamiento de $\mathcal{C}_1$. Esta nueva serie subnormal tiene $nm + 1$ subgrupos, no necesariamente diferentes.

El siguiente diagrama ilustra las contenencias entre los subgrupos considerados en la demostración.

Ahora para cada $j \in \{0, 1, \ldots, m-1\}$ definimos

$$V_{j,i} := V_j(V_{j+1} \cap U_i), \quad i \in \{0, 1, \ldots, n\}.$$

[2]Otto Schreier (Vienna, 1901-Hamburg, 1929), matemático austriaco. Realizó grandes contribuciones en la teoría de grupos.

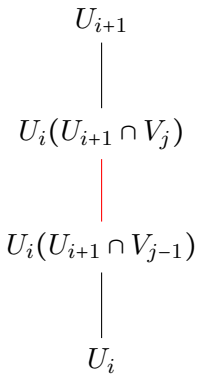


Figura 9.2: Refinamiento

Note que

$$V_{j,n} = V_{j+1} = V_{j+1,0}.$$

Se obtiene entonces una serie subnormal $\mathcal{C}_2'$, la cual es un refinamiento de $\mathcal{C}_2$ y está conformada por $nm+1$ subgrupos.

Usando nuevamente el lema de Zassenhaus se sigue que

$$\begin{aligned} U_{i,j+1}/U_{i,j} &= U_i(U_{i+1} \cap V_{j+1})/U_i(U_{i+1} \cap V_j) \\ &\cong V_j(V_{j+1} \cap U_{i+1})/V_j(V_{j+1} \cap U_i) \\ &= V_{j,i+1}/V_{j,i}. \end{aligned} \tag{9.1}$$

Para indexar las cadenas $\mathcal{C}_1'$ y $\mathcal{C}_2'$ fueron utilizados, respectivamente, los conjuntos

$$\begin{aligned} I &= \{(i,j) \mid 0 \leq i \leq n-1,\ 0 \leq j \leq m-1\} \cup \{(n,0)\} \\ J &= \{(r,s) \mid 0 \leq r \leq m-1,\ 0 \leq s \leq n-1\} \cup \{(m,0)\}. \end{aligned}$$

Sea K el conjunto definido por

$$K = \{k \in \mathbb{Z} \mid 0 \leq k \leq nm\}.$$

Se verifica que $|I| = |J| = |K| = nm+1$. Entonces podemos usar K para indexar las cadenas $\mathcal{C}_1'$ y $\mathcal{C}_2'$. Para ello procedamos de la siguiente manera:

$$\begin{aligned} I \ni (i,j) &\mapsto im + j \in K \\ (n,0) &\mapsto nm \\ J \ni (r,s) &\mapsto rn + s \in K \\ (m,0) &\mapsto mn. \end{aligned}$$

En esta nueva notación, para $(i,j) \in I$ y $(r,s) \in J$ tenemos que

$$\begin{aligned} U_{i,j} &= U_{im+j} \\ U_{n,0} &= U_{nm} \\ V_{r,s} &= V_{rn+s} \\ V_{m,0} &= V_{mn}. \end{aligned}$$

Sea ahora $\Omega = \{0, 1, \ldots, nm-1\}$, y como es usual, notemos con $\mathrm{Sym}(\Omega)$ el grupo de las biyecciones de Ω.

Si $k \in \Omega$, entonces existe $(i,j) \in I$ tal que $k = im + j$. Si definimos $\pi : \Omega \longrightarrow \Omega$ mediante

$$\pi(k) = \pi(im + j) = jn + i,$$

entonces se verifica que $\pi \in \mathrm{Sym}(\Omega)$.

Demostramos que π es inyectiva. Para ello supongamos que $\pi(im + j) = \pi(i'm + j')$. Entonces $jn + i = j'n + i'$ o, equivalentemente,

$$(j - j')n = i' - i. \tag{9.2}$$

Sin perder generalidad supongamos que $j \geq j'$. Si $j \neq j'$, entonces (9.2) implicaría que

$$n < (j - j')n = i' - i \leq n - 1 < n,$$

lo cual es contradictorio. En consecuencia, $j = j'$ y $i = i'$, con lo cual se tiene la inyectividad de π. Dado que Ω es finito se tiene que $\pi \in \mathrm{Sym}(\Omega)$.

Finalmente,

$$\begin{aligned} U_{k+1}/U_k &= U_{im+j+1}/U_{im+j} \\ &= U_{i,j+1}/U_{i,j}. \end{aligned}$$

y

$$\begin{aligned} V_{\pi(k)+1}/V_{\pi(k)} &= V_{jn+i+1}/V_{jn+i} \\ &= V_{j,i+1}/V_{j,i}. \end{aligned}$$

Usando (9.1) se sigue que

$$U_{k+1}/U_k \cong V_{\pi(k)+1}/V_{\pi(k)},$$

para $k \in \Omega$, con lo cual se completa la prueba. □

9.3 El teorema de Jordan-Hölder

9.3.1 Definición. Una serie subnormal de G, digamos

$$(\mathcal{C}) \quad 1 = U_0 \subseteq U_1 \subseteq \cdots \subseteq U_n = G,$$

se denomina una `serie de composición` de G si sus correspondientes factores son grupos simples. En este caso, cada cociente U_{i+1}/U_i se denomina un `factor de composición` de G.

9.3.2 Definición. Una cadena normal de G, digamos

$$(\mathcal{C}) \quad 1 = U_0 \subset U_1 \subset \cdots \subset U_n = G,$$

se denomina una `serie principal` de G si para todo $i \in \{1, \ldots, n-1\}$ se verifica que U_{i+1}/U_i es un subgrupo normal minimal de G/U_i. Los grupos cocientes U_{i+1}/U_i se denominan `factores principales` de G. Se dice que un factor principal H/K de G es `central` en G si $H/K \leq Z(G/K)$.

9.3.3 Ejemplos. (1) Todo grupo finito admite una serie de composición.

(2) La cadena $(1) \trianglelefteq \langle (12)(34) \rangle \trianglelefteq V_4 \trianglelefteq \mathrm{Alt}(4) \trianglelefteq \mathrm{Sym}(4)$ es una serie de composición de $\mathrm{Sym}(4)$.

(3) El grupo aditivo $\mathbb{Z}$ no admite una serie de composición. En efecto, toda serie subnormal $\{0\} \trianglelefteq n_1\mathbb{Z} \trianglelefteq \cdots \trianglelefteq n_k\mathbb{Z} \trianglelefteq \mathbb{Z}$ puede refinarse con $\{0\} \trianglelefteq n_1^2\mathbb{Z} \trianglelefteq n_1\mathbb{Z} \trianglelefteq \cdots \trianglelefteq n_k\mathbb{Z} \trianglelefteq \mathbb{Z}$.

El siguiente resultado se intuye en los trabajos de Camille Jordan[3], no obstante su demostración se atribuye a Otto Hölder[4].

9.3.4 Teorema. (Jordan, 1869 - Hölder, 1889) Supongamos que G admite una serie de composición. Entonces cualquier par de series de composición de G son equivalentes.

Demostración. Sean

$$(\mathcal{C}) \quad 1 = U_0 \subseteq U_1 \subseteq \cdots \subseteq U_n = G$$

[3]Marie Ennemond Camille Jordan (Lyon, 1838, París, 1922), matemático e ingeniero francés. Destacado por sus aportes en la teoría de grupos y en las ecuaciones algebraicas.

[4]Otto Ludwig Hölder (Stuttgart, 1859-Leipzig, 1937), matemático alemán.Trabajó en covergencia de series de Fourier y en 1884 descubrió la desigualdad, ahora conocida con su nombre. Se interesó además en teoría de grupos y demostró la unicidad de los grupos factores en las series de composición de un grupo.

y

$$(\mathcal{C}') \quad 1 = V_0 \subseteq V_1 \subseteq \cdots \subseteq V_m = G$$

dos series de composición de G. Usando el teorema de Schreier podemos afirmar que $\mathcal{C}$ y $\mathcal{C}'$ admiten refinamientos subnormales equivalentes.

Dado que para cada $i \in \{0, 1, \ldots, n-1\}$ y cada $j \in \{0, 1, \ldots, m-1\}$ se verifica que $U_i \lhd U_{i+1}$ y $V_j \lhd V_{j+1}$, dichos refinamientos no son propios. Es decir, estos coinciden con las series de composición originales. Por lo tanto, deben ser equivalentes. □

9.3.5 Corolario. Supongamos que G admite una serie de composición y $N \triangleleft G$. Entonces N es elemento de alguna serie de composición de G.

Demostración. Consideremos la cadena

$$(\mathcal{C}) \quad 1 < N < G. \tag{9.3}$$

Es claro que esta es una serie subnormal de G. Sea ahora

$$(\mathcal{C}') \quad 1 = U_0 \subseteq U_1 \subseteq \cdots \subseteq U_n = G$$

una serie de composición de G. Del teorema de Schreier se sigue nuevamente que $\mathcal{C}$ y $\mathcal{C}'$ admiten refinamientos equivalentes. Dado que $\mathcal{C}'$ es una serie de composición, el refinamiento de $\mathcal{C}$ también lo es. □

9.3.6 Corolario. (Teorema fundamental de la aritmética) Sea $n \in \mathbb{Z}$ con $n > 1$. Entonces existen números primos únicos $p_1, \ldots, p_k$ con $p_1 < \cdots < p_k$ y enteros positivos $a_1, \ldots, a_k$ tales que $n = p_1^{a_1} \cdots p_k^{a_k}$.

Demostración. Para todo $n \in \mathbb{Z}$ con $n > 1$ existe (salvo isomorfía) un grupo cíclico de orden n. Denotémoslo con C_n y digamos que $\mathrm{C}_n = \langle g \rangle$. Todo subgrupo de C_n es normal y para cada $d \mid n$ se verifica que existe un único subgrupo de orden d.

Sea d el mayor divisór propio de n y U_1 el único subgrupo de C_n cuyo orden es d. Entonces el grupo G/U_1 es cíclico y simple. Por lo tanto, con orden un número primo. Aplicando esta construcción al grupo U_1 podemos construir una serie de composición $G = U_0 \supseteq U_1 \supseteq \cdots \supseteq U_r = 1$, con U_{i-1}/U_i de orden primo, digamos p_i, $i = 1, \ldots, r$. Entonces

$$\begin{aligned} n &= |G| \\ &= |G/U_1||U_1| \\ &= |G/U_1||U_1/U_2| \cdots |U_{r-1}/U_r||U_r| \\ &= p_1 p_2 \ldots p_{r-1} 1. \end{aligned}$$

La unicidad de los números primos se sigue del teorema de Jordan-Hölder aplicado al grupo G. □

9.4 Series de composición y grupos solubles

En lo que sigue presentamos la relación que existe entre grupos solubles y series de composición.

9.4.1 Lema. Todo refinamiento de una serie normal con factores abelianos de un grupo G es una serie normal con factores abelianos.

Demostración. Sea

$$(\mathcal{C}) \quad 1 = U_0 \leq U_1 \leq \cdots \leq U_n = G$$

una serie normal con factores abelianos. Es suficiente demostrar que en el refinamiento

$$(\mathcal{C}') \quad 1 = U_0 \leq U_1 \leq \cdots \leq U_i \leq N \leq U_{i+1} \leq \cdots \leq U_n = G$$

los factores N/U_i y U_{i+1}/N son abelianos. Dado que $N/U_i \leq U_{i+1}/U_i$, se tiene que N/U_i es abeliano. Utilizando el tercer teorema de isomorfía se tiene que

$$(U_{i+1}/U_i)/(N/U_i) \cong U_{i+1}/N,$$

con lo cual se tiene la otra afirmación. □

9.4.2 Teorema. Sea G un grupo que admite una serie de composición. Entonces G es soluble si y solo si los factores de composición de G tienen orden un número primo.

Demostración. Sea G un grupo soluble que admite una serie de composición. Entonces del teorema 7.3.6 se tiene que G admite también una serie normal con factores abelianos. Del teorema de Schreier se sigue que ambas cadenas pueden refinarse y obtener series normales equivalentes. Del lema 9.4.1 se tiene que estos refinamientos equivalentes tienen factores abelianos.

Dado que los refinamientos de series de composición son triviales, se tiene que la serie de composición de G tiene factores abelianos. Entonces los factores de composición son grupos simples y abelianos. En consecuencia, estos son grupos cíclicos y con orden un número primo.

Recíprocamente, sea G un grupo que admite una serie de composición, en la cual los factores de composición tienen orden un número primo. Entonces G tiene una serie normal con afactores abelianos y, por lo tanto, G es soluble. □

9.4.3 Corolario. Un grupo soluble G admite una serie de composición si y solo si G es finito.

DEMOSTRACIÓN. Si G es finito, entonces es claro que G admite una serie de composición.

Recíprocamente, sea G un grupo soluble que admite una serie de composición, digamos

$$(\mathcal{C}) \quad 1 = U_0 \leq U_1 \leq \cdots \leq U_n = G.$$

Del teorema anterior se sigue que para todo $i \in \{0, \ldots, n-1\}$

$$|U_{i+1}| = |U_{i+1}/U_i||U_i| = p|U_i|$$

para algún número primo p. En consecuencia, $|G| = p_1 \cdots p_{n-1}$, donde cada p_i es un número primo. Es decir, G es finito. □

9.5 Subgrupos normales minimales

En esta sección consideramos los subgrupos normales minimales de un grupo soluble G. Estos subgrupos juegan un papel importante en las pruebas de los teoremas de P. Hall sobre la generalización de la teoría de Sylow en el contexto de los grupos solubles.

9.5.1 Definición. Sea G un grupo y $N \trianglelefteq G$. Decimos que N es un subgrupo normal minimal de G, notado $N \cdot \trianglelefteq\ G$, si $N \neq 1$ y, si $1 \leq K \leq N$ con $K \trianglelefteq G$, entonces $K = 1$ o $K = N$.

9.5.2 Ejemplos. (1) Si G es simple, entonces G es su único subgrupo normal minimal.

(2) Si $G = \mathrm{Sym}(4)$, entonces $N = \{(1), (12)(34), (13)(24), (14)(23)\}$ es un subgrupo normal minimal de G.

9.5.3 Observación. En el ejemplo anterior (2) se tiene que G es un grupo soluble y además se tiene que $N \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ es un grupo abeliano elemental. Demostramos en esta sección que esto siempre es verdadero para grupos solubles finitos. Fuera del contexto soluble esta afirmación es falsa. Por ejemplo, consideremos el grupo $G = \mathrm{Sym}(5)$. El único subgrupo normal no trivial de G es $\mathrm{Alt}(5)$, por lo tanto, un subgrupo normal minimal. Es claro que $\mathrm{Alt}(5)$ no es abeliano elemental.

9.5.4 Lema. Sea G un grupo. Si $N_1, \ldots, N_r$ son subgrupos normales minimales de G, entonces $K := \langle N_1, \ldots, N_r \rangle$ es el producto directo de algunos de los N_j.

DEMOSTRACIÓN. Definamos el conjunto $\mathcal{N}$ de la siguiente manera:

$$\mathcal{N} := \{N \leq K \mid N \text{ es producto directo de algunos de los } N_j\}.$$

Del teorema 1.2.24 se sigue que $\mathcal{N} \neq \varnothing$. Sea $N \in \mathcal{N}$ con el número de factores N_i maximal. Sin perder generalidad, supongamos que

$$N = N_1 \times \cdots \times N_s.$$

Si $N = K$, entonces se tiene el resultado. Supongamos que $N \neq K$. Es decir, existe N_j con $N_j \nleq N$. Entonces

$$N_j \cap N \trianglelefteq G \quad \text{y} \quad N_j \cap N < N_j.$$

Dado que $N_j \cdot \trianglelefteq\ G$, se tiene que $N_j \cap N = 1$. Por lo tanto,

$$NN_j = N \times N_j = N_1 \times \cdots \times N_s \times N_j \in \mathcal{N},$$

lo cual contradice la escogencia de N. En consecuencia, $N = K$. □

9.5.5 Definición. Un grupo finito se denomina `característico simple` si no admite subgrupos característicos no triviales.

9.5.6 Teorema. Si G es un grupo característico simple, entonces G es un grupo simple o es el producto directo de grupos simples isomorfos.

Demostración. Sea G un grupo característico simple, el cual no es un grupo simple y sea $N \cdot \trianglelefteq\ G$. Entonces para todo $\alpha \in \mathrm{Aut}(G)$ se verifica que $\alpha(N) \cdot \trianglelefteq\ G$. Por otro lado, sea

$$K := \langle \alpha(N) \mid \alpha \in \mathrm{Aut}(G) \rangle \leq G.$$

Se verifica que $1 \neq K$ char G. Dado que G es característico simple, se tiene que $G = K$. Del lema 9.5.4 se sigue que existen $\alpha_1, \ldots, \alpha_s \in \mathrm{Aut}(G)$ tales que

$$G = \alpha_1(N) \times \cdots \times \alpha_s(N).$$

Es claro que para todo $i, j \in \{1, \ldots, s\}$ se tiene que $\alpha_i(N) \cong \alpha_j(N)$.

Demostramos ahora que cada $\alpha_j(N)$ es simple. Para ello sean $M \trianglelefteq \alpha_j(N)$, $m \in M$ y $g = g_1 \cdots g_s \in G$. Dado que para $i \neq j$ se verifica que cada elemento de $\alpha_i(N)$ conmuta con cada elemento de $\alpha_j(N)$, se sigue que

$$gmg^{-1} = g_j m g_j^{-1} \in M.$$

Esto demuestra que $M \trianglelefteq G$. Dado que $\alpha_j(N) \cdot \trianglelefteq\ G$, se sigue que $M = 1$ o $M = \alpha_1(N)$ y se tiene el resultado. □

9.5.7 Teorema. Sea G un grupo finito y $N \cdot \trianglelefteq\ G$. Entonces N es un p-grupo abeliano elemental para algún primo p o N es el producto directo de grupos simples, no abelianos isomorfos.

Demostración. Si M char N, entonces, dado que $N \trianglelefteq G$, se sigue que $M \trianglelefteq G$. Por lo tanto, $M = 1$ o $M = N$. Es decir, N es característico simple. Del teorema 9.5.6 se sigue que

$$N = N_1 \times \cdots \times N_r,$$

donde los N_j son grupos simples isomorfos.

Si N_j es abeliano, entonces $|N_j| = p$ para algún número primo p y se tiene que N es un grupo abeliano elemental. □

9.5.8 Teorema. Sea G un grupo finito soluble. Entonces

(1) Todo subgrupo normal minimal de G es p-grupo abeliano elemental para algún primo p.

(2) Si $M \lessdot G$, entonces $|G : M|$ es potencia de algún número primo. El recíproco de esta afirmación es en general falso.

Demostración. (1) Si $N \trianglelefteq G$, entonces del teorema anterior es N un p-grupo abeliano elemental para algún primo p o bien

$$N = N_1 \times \cdots \times N_r,$$

donde los N_j son grupos simples no abelianos e isomorfos. Dado que G es soluble, se tiene que N_1 también lo es. Si N_1 fuese simple no abeliano, entonces $1 \neq N_1' = N_1$, lo cual contradice la solubilidad de N_1. Por lo tanto, la segunda opción no se tiene.

(2) Procedemos por inducción sobre $|G|$. Sean $N \trianglelefteq G$ y $M \lessdot G$. De (1) se sigue que $|N| = p^a$ para algún número primo p y algún $a \in \mathbb{N}$. Diferenciamos dos casos:

`Caso 1.` Si $N \leq M$, entonces $M/N \lessdot G/N$. Dado que G/N es soluble, aplicando la hipótesis de inducción se tiene que

$$\underbrace{|G/N : M/N|}_{p\text{–potencia}} = |G : M|.$$

`Caso 2.` Si $N \nleq M$, entonces $M \cap N < N$, por lo tanto, $M \cap N = 1$. Por otro lado, $M < MN \leq G$, en consecuencia, por la maximalidad de M se tiene que $G = MN$. Entonces

$$|G : M| = |MN : M| = |N : N \cap M| = |N|,$$

el cual es una p-potencia. □

Dado que los factores principales de G son grupos característicos y simples, del teorema 9.5.6 se sigue que G es soluble si y solo si todos los factores principales de G son productos directos de grupos isomorfos con orden un número primo.

9.5.9 Observaciones. Sea G un grupo finito.

1. Es posible que todos los subgrupos maximales de G tengan como índice potencia de un número primo y sin embargo G no sea soluble. El ejemplo más famoso es

$$G = \mathrm{PSL}(2,7) = \mathrm{SL}(2,7)/Z(\mathrm{SL}(2,7)).$$

   G es un grupo simple, no abeliano con $|G| = 168$ y todos sus subgrupos maximales tienen índice 7 u 8.

2. P. Hall demostró que si todos los subgrupos maximales de G tienen índice un número primo o el cuadrado de un número primo, entonces G es soluble. Una demostración de este resultado se encuentra en [9] VI (9.4).

3. En 1904 W. Burnside[5] demostró que para números primos arbitrarios p y q y $a, b \in \mathbb{N}_0$ cualquier grupo con orden $p^a q^b$ es soluble. Conjeturó que cualquier grupo de orden impar debería ser soluble.

4. W. Feit[6] y J. Thompson[7] demostraron en 1963 la conjetura de de Burnside. Este resultado fue publicado en la revista *Pacific Journal of Mathematics*. La prueba de este teorema consta de unas 274 páginas.

5. J. Thompson demostraró que si $3 \nmid |G|$ o $5 \nmid |G|$, entonces G es soluble. Por sus múltiples aportes a la teoría de grupos finitos recibió en 1970 la Medalla Field.

[5] William Burnside (1852, Londres-1927 West Wickham), matemático inglés. Burnside es conocido por su trabajo en teoría de grupos finitos, a la que se dedicó a partir de 1893. En 1897 publicó su mayor obra *Teoría de los grupos de orden finito*, el primer libro de texto en inglés sobre el tema, que no era muy popular entre los matemáticos ingleses de la época.

[6] Walter Feit (1930-2004) fue un matemático estadounidense que trabajó en teoría de grupos finitos y teoría de representaciones. Sus contribuciones sirvieron posteriormente para usarse en álgebra, geometría, topología, teoría de números y lógica.

[7] John Griggs Thompson (13 de octubre de 1932) es un matemático de la Universidad de Florida conocido por su trabajo en el campo de los grupos finitos. Fue galardonado con la Medalla Fields en 1970, el Premio Wolf en 1992 y el Premio Abel 2008.

CAPÍTULO 10

NILPOTENCIA Y SOLUBILIDAD - PARTE 2

> Hizo fundir asimismo un mar de diez codos de un lado al otro, perfectamente redondo; su altura era de cinco codos, y lo ceñía alrededor un cordón de treinta codos. Y rodeaban aquel mar por debajo de su borde alrededor unas bolas como calabazas, diez en cada codo, que ceñían el mar alrededor en dos filas, las cuales habían sido fundidas cuando el mar fue fundido.
>
> (1 Reyes 7: 23-24.)

10.1 El subgrupo de Frattini

En la teoría de grupos el subgrupo de Frattini juega un papel importante, por ejemplo con la ayuda de este se puede estudiar la estructura de p-grupos finitos. Este subgrupo lleva este nombre en honor del matemático italiano G. Frattini[1].

10.1.1 Definición. Sea $G \neq 1$. Definimos su `subgrupo de Frattini`, notado con $\Phi(G)$, como la intersección de todos sus subgrupos maximales. Esto es,

$$\Phi(G) := \bigcap \{M \mid M \lessdot G\}.$$

[1]Giovanni Frattini (1852-1925), matemático italiano. Conocido por sus múltiples contribuciones en la teoria de grupos. Además de la teoría de grupos también se ocupó de la geometría diferencial y la teoría de números de formas cuadráticas binarias.

Definimos además $\Phi(1) := 1$.

10.1.2 Ejemplos. (1) $\Phi(\mathbb{Z}) = \{0\}$.

(2) $\Phi(\mathbb{Z}_p^\infty) = \mathbb{Z}_p^\infty$.

(3) $\Phi(\mathrm{Sym}(3)) = 1$.

(4) Sea $G = \langle g \rangle$ con $|G| = p^2$ y p un número primo. Entonces $\Phi(G) = \langle g^p \rangle$.

(5) Si $G = D_8$, entonces $\Phi(G)$ es uno de sus subgrupos de orden 2.

10.1.3 Lema. Sea G finito, $N \trianglelefteq G$ y $X \subseteq G$. Entonces

(1) $\Phi(G)$ char G.

(2) $\langle X, \Phi(G) \rangle = G$ si y solo si $\langle X \rangle = G$.

(3) Existe $H < G$ con $G = HN$ si y solo si $N \nleq \Phi(G)$.

Demostración. (1) Sean $\alpha \in \mathrm{Aut}(G)$ y $M \lessdot G$. Se verifica sin dificultades que $\alpha(M) \lessdot G$. Por lo tanto,

$$\begin{aligned} \alpha(\Phi(G)) &= \alpha(\bigcap\{M \mid M \lessdot G\}) \\ &\subseteq \bigcap\{\alpha(M) \mid M \lessdot G\} \\ &= \Phi(G). \end{aligned}$$

(2) Si $\langle X \rangle = G$, entonces es inmediato que $\langle X, \Phi(G) \rangle = G$.

Recíprocamente, supongamos que $\langle X, \Phi(G) \rangle = G$, y supongamos además que $\langle X \rangle < G$. Entonces existiría $M \lessdot G$ con $\langle X \rangle \leq M$ y, en consecuencia, dado que $\Phi(G) \leq M$, se tendría que

$$\langle X, \Phi(G) \rangle = G \leq M,$$

lo cual es una contradicción. Por lo tanto, $\langle X \rangle = G$.

(3) Supongamos que existe $H < G$ con $G = HN$, y supongamos además que $N \leq \Phi(G)$. Entonces

$$G = HN = \Phi(G)H = \langle \Phi(G), H \rangle = \langle H \rangle = H,$$

lo cual es una contradicción. En consecuencia, $N \nleq \Phi(G)$.

Recíprocamente, supongamos que $N \nleq \Phi(G)$. Entonces existe $H \lessdot G$ con $N \leq H$. De $H < HN \leq G$ se sigue que $HN = G$. □

10.1.4 Observación. Un elemento de un grupo $G \neq 1$ se denomina no-generador si en todo conjunto generador de G que lo contenga resulta redundante. Entonces del lema anterior se tiene una nueva caracterización del subgrupo $\Phi(G)$. Este puede verse como el conjunto de todos los elementos no-generadores de G.

10.1.5 Lema. Sea G finito, $N \trianglelefteq G$ y $U \leq G$. Entonces

(1) Si $N \leq \Phi(U)$, entonces $N \leq \Phi(G)$.

(2) $\Phi(N) \leq \Phi(G)$. En particular $\Phi(N) \trianglelefteq \Phi(G)$.

(3) En general, si $H < G$, no siempre se verifica que $\Phi(H) \leq \Phi(G)$.

Demostración. (1) Supongamos que $N \leq \Phi(U)$ y que $N \nleq \Phi(G)$. Entonces existiría $M \lneq G$ con $N \nleq M$ y, en consecuencia, dado que $M < NM$, se tendría que $G = MN$. Dado que $N \leq \Phi(U)$, se sigue que $N \leq U$ y además

$$U = U \cap MN = (U \cap M)N = U \cap M \leq M.$$

Por lo tanto, $N \leq \Phi(U) \leq M$, lo cual es una contradicción.

(2) Dado que $\Phi(N)$ char N y $N \trianglelefteq G$, se tiene que $\Phi(N) \trianglelefteq G$. Usando (1) con $N = \Phi(N)$ y $U = N$ se tiene la afirmación.

(3) Se deja como ejercicio. □

10.1.6 Lema. Sea G finito y $N \trianglelefteq G$. Entonces

(1) Si $\Phi(G)N/N \leq \Phi(G/N)$.

(2) Si $N \leq \Phi(G)$, entonces $\Phi(G)/N = \Phi(G/N)$.

(3) En general, no siempre se verifica que $\Phi(G)N/N = \Phi(G/N)$.

Demostración. (1) Del tercer teorema de isomorfía y del principio de correspondencia se sigue que todo subgrupo maximal de G/N es de la forma M/N, con $M \lneq G$ y $N \leq M$. Por lo tanto, para cada uno de estos subgrupos M se verifica que $\Phi(G) \leq M$. Entonces

$$\Phi(G)N/N \leq M/N$$

y consecuentemente,

$$\Phi(G)N/N \leq \bigcap\{M/N \mid N \leq M \lneq G\} = \Phi(G/N).$$

(2) Si $N \leq \Phi(G)$, entonces de (1) se sigue que

$$\Phi(G)/N = \Phi(G)N/N \leq \Phi(G/N).$$

Por otro lado, si $N \leq \Phi(G)$, entonces $N \leq M$ para todo $M \lessdot G$. Por lo tanto, $\Phi(G/N) \leq M/N$ para todo $M \lessdot G$. Así,

$$\Phi(G/N) \leq \bigcap\{M/N \mid M \lessdot G\} = \Phi(G)/N.$$

(3) Se deja como ejercicio. □

10.1.7 Lema. (Frattini, 1885) Sea G un grupo finito. Entonces

(1) $\Phi(G)$ es nilpotente.

(2) Si $G/\Phi(G)$ es nilpotente, entonces G es nilpotente.

(3) $G' \cap Z(G) \leq \Phi(G)$.

Demostración. (1) Sea $P \in \mathrm{Syl}_p(\Phi(G))$. Dado que $\Phi(G)$ char G, en particular se tiene que $\Phi(G) \trianglelefteq G$. Del argumento de Frattini II se sigue que

$$G = N_G(P)\Phi(G) = \langle N_G(P), \Phi(G)\rangle = \langle N_G(P)\rangle = N_G(P).$$

Esto demuestra que $P \trianglelefteq G$, por lo tanto, $P \trianglelefteq \Phi(G)$. Del teorema 8.2.10 se sigue que $\Phi(G)$ es nilpotente.

(2) Supongamos que $G/\Phi(G)$ es nilpotente y sea $P \in \mathrm{Syl}_p(G)$. Entonces $P\Phi(G)/\Phi(G) \in \mathrm{Syl}_p(G/\Phi(G))$. Entonces $P\Phi(G)/\Phi(G) \trianglelefteq G/\Phi(G)$ y, en consecuencia, $P\Phi(G) \trianglelefteq G$. Usando nuevamente el argumento de Frattini II se tiene que

$$G = N_G(P)P\Phi(G) = N_G(P)\Phi(G) = N_G(P).$$

En consecuencia, $P \trianglelefteq G$ y nuevamente del teorema 8.2.10 se sigue que G es nilpotente.

(3) Supongamos que $N := G' \cap Z(G) \nleq \Phi(G)$. Entonces del lema 10.1.3 (3) se sigue que existe $H < G$ con $G = HN$; más aún, el subgrupo H puede tomarse de tal forma que $H \lessdot G$.

Por otro lado, para $n \in N$ y $h \in H$ se verifica que

$$nhHh^{-1}n^{-1} = nHn^{-1} = H.$$

Por lo cual, $H \trianglelefteq G$ y se tiene que el grupo cociente G/H es cíclico de orden primo. En particular G/H es abeliano y del lema 7.1.7 se sigue que $G' \leq H$. Por lo tanto, $N \leq H$ y se tendría que $G = HN \leq H$, lo cual es una contradicción. □

10.1.8 Teorema. (H. Wielandt, 1937) Un grupo finito G es nilpotente si y solo si $G' \subseteq \Phi(G)$.

DEMOSTRACIÓN. Si G es un grupo finito nilpotente, entonces del teorema 8.2.12 se sigue que todo subgrupo maximal M de G es normal en G. Por lo tanto, G/M tiene orden primo, y en particular G/M es abeliano, lo cual trae como consecuencia que $G' \leq M$. Es decir, $G' \subseteq \Phi(G)$.

Recíprocamente, supongamos que $G' \subseteq \Phi(G)$. Entonces $G/\Phi(G)$ es abeliano y por lo tanto, nilpotente. La conclusión se sigue del teorema 10.1.7 (2). □

Una consecuencia inmediata de los lema 7.1.7, 10.1.7 (2) y del teorema 10.1.8 es el siguiente resultado.

10.1.9 Corolario. Sea G un grupo finito. Entonces las siguientes afirmaciones son equivalentes:

(1) G es nilpotente.

(2) $G' \leq \Phi(G)$.

(3) $G/\Phi(G)$ es abeliano.

(4) $G/\Phi(G)$ es nilpotente.

Recordemos que si G es un p-grupo finito, entonces este se denomina `abeliano elemental` si $g^p = 1$ para todo $g \in G$.

10.1.10 Observación. Sea G un p-grupo abeliano elemental. Es decir, $G = \langle g_1 \rangle \times \cdots \times \langle g_n \rangle$, con $\text{ord}(g_j) = p$ para todo $j = 1, 2, \ldots, n$. Si definimos la siguiente multiplicación por escalar

$$(k + p\mathbb{Z})x = x^k \text{ para todo } x \in G,\ k \in \mathbb{Z},$$

entonces G adquiere la estructura de espacio vectorial sobre $\mathbb{Z}_p$. Entonces existe $n \in \mathbb{N}$ tal que G es isomorfo al espacio vectorial $\mathbb{Z}_p^n$ de dimensión n sobre el cuerpo $\mathbb{Z}_p$.

Claramente, todo subgrupo de G es un subespacio vectorial de G y cada homomorfismo entre p-grupos abelianos elementales es una función $\mathbb{Z}_p$-lineal. En particular, para cada subconjunto X de G se verifica que $\langle X \rangle = \langle X \rangle_{\mathbb{Z}_p}$.

10.1.11 Lema. Sea G un p-grupo finito y $N \trianglelefteq G$. Si G/N es un p-grupo abeliano elemental, entonces $\Phi(G) \subseteq N$. En consecuencia, si G un p-grupo finito, entonces $\Phi(G)$ es el subgrupo normal más pequeño de G con grupo cociente abeliano elemental.

Demostración. Sea $N \trianglelefteq G$ con G/N un p-grupo abeliano elemental, y supongamos además que $\Phi(G) \nsubseteq N$. Entonces existe $x \in \Phi(G) \setminus N$.

Dado que G/N es un p-grupo abeliano elemental, se verifica que G/N es isomorfo al grupo aditivo del espacio vectorial n-dimensional $\mathbb{Z}_p^n$ para algún $n \in \mathbb{N}$. Entonces existe una base sobre $\mathbb{Z}_p$ de la forma

$$\mathcal{B} = (xN, x_2N, \ldots, x_nN).$$

Entonces $G = \langle x, x_2, \ldots, x_n, N\rangle$, y dado que $x \in \Phi(G)$, se verifica que $G = \langle x_2, \ldots, x_n, N\rangle$, lo cual trae como consecuencia que

$$G/N = \langle x_2N, \ldots, x_nN\rangle,$$

lo cual es una contradicción. Esto demuestra que $\Phi(G) \leq N$. □

10.1.12 Teorema. Sea G un p-grupo. Entonces

(1) $\Phi(G) = G'G^p$, donde $G^p = \langle g^p \mid g \in G\rangle$. O, equivalentemente,

$$\Phi(G) = \langle [x, y], z^p \mid x, y, z \in G\rangle.$$

En particular $G/\Phi(G)$ es un p-grupo abeliano elemental.

(2) Si $p = 2$, entonces $\Phi(G) = G^2$. En este caso el subgrupo de Frattini de G es generado por lo cuadrados de los elementos de G.

(3) Si $U \leq G$, entonces $\Phi(U) \leq \Phi(G)$.

(4) Si $N \trianglelefteq G$, entonces $\Phi(G)N/N = \Phi(G/N)$.

Demostración. (1) Sea $M \lessdot G$. Dado que G es un p-grupo, se verifica que G es un grupo nilpotente y, en consecuencia, $M \lhd G$. De la maximalidad de M se sigue que $|G : M| = p$ y, consecuentemente, G/M es cíclico. En particular G/H es abeliano y del lema 7.1.7 se sigue que $G' \leq M$.

Por otro lado, para demostrar que $G^p \leq M$, sea $g \in G$. Entonces

$$M = (gM)^p = g^pM,$$

con lo cual se tiene que $g^p \in M$ para todo $g \in G$. Así que, en resumen, se tiene que $G'G^p \leq M$ para todo subgrupo maximal M de G. En consecuencia, $G'G^p \leq \Phi(G)$.

Demostramos a continuación que $\Phi(G) \leq G'G^p$.

Dado que $G' \leq G'G^p \leq G$, del lema 7.1.7 se sigue que $G'G^p \trianglelefteq G$, y además que $G/G'G^p$ es abeliano.

Se verifica que todo elemento no trivial de $G/G'G^p$ tiene orden p. En efecto, si $g \in G$, entonces

$$(gG'G^p)^p = g^pG'G^p = G'G^p.$$

Esto demuestra que $G/G'G^p$ es un p-grupo abeliano elemental y del lema anterior se sigue que $\Phi(G) \leq G'G^p$.

(2) Es suficiente demostrar que todo conmutador puede expresarse como producto de cuadrados. Sean $g, h \in G$. Entonces

$$[g,h] = ghg^{-1}h^{-1} = (ghg^{-1})^2g^2(g^{-1}h^{-1})^2.$$

(3) Como consecuencia de (1) se tiene que

$$\Phi(U) = U'U^p \leq G'G^p = \Phi(G).$$

(4) Nuevamente, como consecuencia de (1) se tiene que

$$\begin{aligned}\Phi(G/N) &= (G/N)'(G/N)^2\\ &= (G'N/N)(G^N/N)\\ &= G'G^2N/N\\ &= \Phi(G)N/N. \qquad \square\end{aligned}$$

10.1.13 Teorema de la base de Burnside. Sea G un p-grupo finito con $|G/\Phi(G)| = p^d$. Entonces G tiene un conjunto generador con d elementos y ningún subconjunto de G con menos de d elementos genera a G. Además todo elemento de $G \setminus \Phi(G)$ pertenece a algún conjunto minimal de generadores.

Demostración. Note que $G/\Phi(G)$ es un p-grupo abeliano elemental y por lo tanto, puede verse como un espacio vectorial sobre $\mathbb{Z}_p$ con dimensión d. Entonces

$$\begin{aligned}G/\Phi(G) = \langle x_1\Phi(G), \ldots, x_n\Phi(G)\rangle &\Leftrightarrow G = \langle x_1, \ldots, x_n, \Phi(G)\rangle\\ &\Leftrightarrow G = \langle x_1, \ldots, x_n\rangle.\end{aligned}$$

Sea $\{x_1, \ldots, x_n\}$ un conjunto minimal generador de G. Entonces de lo anterior se sigue que $G/\Phi(G) = \langle x_1\Phi(G), \ldots, x_n\Phi(G)\rangle$, y dado que $G/\Phi(G)$ como espacio vectorial sobre $\mathbb{Z}_p$ tiene dimensión d, se verifica que $d \leq n$. Supongamos que $d < n$. Entonces existe un subconjunto propio de $\{x_1\Phi(G), \ldots, x_n\Phi(G)\}$, el cual también genera a $G/\Phi(G)$. Entonces

el correspondiente subconjunto propio de $\{x_1, \ldots, x_n\}$ generaría a G, lo cual contradice la minimalidad de $\{x_1, \ldots, x_n\}$. En consecuencia, $d = n$.

Sea ahora $x \in G \setminus \Phi(G)$. Entonces $x\Phi(G)$ es un elemento no nulo en el espacio vectorial $G/\Phi(G)$ sobre $\mathbb{Z}_p$ y puede ser extendido a una base

$$\mathcal{B} = (x\Phi(G), x_2\Phi(G), \ldots, x_d\Phi(G)).$$

Se sigue entonces que $\{x, x_2 \ldots, x_d\}$ es un conjunto minimal de generador de G. □

10.1.14 Observaciones. (1) Como consecuencia del teorema de la base de Burnside, si G es un p-grupo finito con $|G/\Phi(G)| = p$, entonces G es cíclico.

(2) Este teorema no es válido para todo grupo nilpotente; por ejemplo, si consideramos el grupo $(\mathbb{Z}_6, +)$, se verifica que los conjuntos $\{[1]\}$ y $\{[2], [3]\}$ son conjuntos minimales generadores.

10.2 El subgrupo de Fitting

10.2.1 Definición. Sea $|G| = p^a m$, p un número primo y $p \nmid m$. Definimos el subgrupo $O_p(G)$ de la siguiente manera:

$$O_p(G) := \bigcap \{P \mid P \in \mathrm{Syl}_p(G)\}.$$

Sea G un grupo finito y p un número primo. Si $N \trianglelefteq G$ y N es un p-grupo, entonces abreviamos diciendo que N es un p-subgrupo normal de G.

10.2.2 Lema. Sea G un grupo como en la definición anterior. Entonces

(1) $O_p(G)$ char G.

(2) $O_p(G) = \langle N \mid N \trianglelefteq G \text{ y } N \text{ es } p\text{-grupo} \rangle$. En particular se verifica que $O_p(G)$ es el p-subgrupo normal más grande de G.

Demostración. (1) De la definición de $O_p(G)$ se sigue inmediatamente que este es un p-grupo. Sea ahora $\alpha \in \mathrm{Aut}(G)$. Entonces

$$\alpha(O_p(G)) \subseteq \bigcap \{\alpha(P) \mid P \in \mathrm{Syl}_p(G)\} = O_p(G).$$

(2) Dado que $O_p(G)$ char G, en particular se verifica que $O_p(G) \trianglelefteq G$, además $O_p(G)$ es un p-grupo. Por lo tanto,

$$O_p(G) \leq \langle N \mid N \trianglelefteq G \text{ y } N \text{ es } p\text{-grupo} \rangle.$$

Demostramos ahora que si $N \trianglelefteq G$ y N es un p-grupo, entonces $N \leq O_p(G)$. En efecto, si $P \in \mathrm{Syl}_p(G)$, entonces NP es un p-subgrupo de G. De la maximalidad de P como p-grupo y de $P \leq PN = NP$ se sigue que $N \leq P$. Por lo tanto, N está contenido en cualquier p-subgrupo de Sylow de G, y así $N \leq O_p(G)$.

Finalmente, note que si N_1 y N_2 son p-subgrupos normales de G, entonces N_1N_2 también es un p-subgrupo normal de G. Recuerde que

$$|N_1N_2| = \frac{|N_1||N_2|}{|N_1 \cap N_2|}$$

y el producto de subgrupos normales es un subgrupo normal. Por lo tanto, el producto de todos los p-subgrupos normales de G es un p-subgrupo normal de G, y de lo anterior se cumple que

$$\langle N \mid N \trianglelefteq G \text{ y } N \text{ es } p\text{-grupo} \rangle \leq O_p(G),$$

con lo cual se tiene la afirmación. □

10.2.3 Definición. Sea G un grupo finito. El subgrupo de `Fitting` de G se nota y define de la siguiente manera:

$$F(G) := \langle O_p(G) \mid \ p \mid |G| \rangle.$$

Es decir, $F(G)$ es el producto de todos los subgrupos $O_p(G)$, donde p recorre el conjunto de todos los divisores primos de $|G|$. Si $G = 1$, entonces se define $F(G) = 1$.

10.2.4 Observación. Sea G finito y $p_1, \ldots, p_r$ todos los divisores primos de $|G|$. Entonces $O_{p_j}(G) \in \mathrm{Syl}_{p_j}(F(G))$ para todo $j = 1, \ldots, r$. Dado que $O_{p_j}(G) \trianglelefteq G$, se tiene que $O_{p_j}(G) \trianglelefteq F(G)$ para todo $j = 1, \ldots, r$. En consecuencia, del teorema 8.2.13 se sigue que $F(G)$ es nilpotente y además

$$F(G) = O_{p_1}(G) \times \cdots \times O_{p_r}(G).$$

Más aún, dado que $O_{p_j}(G)$ char G para todo $j = 1, \ldots, r$, se tiene que $F(G)$ char G.

10.2.5 Teorema. Sea G finito. Entonces

(1) $F(G) = \langle N \mid N \trianglelefteq G \text{ y } N \text{ es nilpotente} \rangle$. En particular $F(G)$ es el subgrupo normal mas grande de G que es nilpotente.

(2) Si $N_1, \ldots, N_r$ son subgrupos normales nilpotentes de G, entonces $\langle N_1, \ldots, N_r \rangle \trianglelefteq G$ y también es nilpotente.

(3) Si N_1 y N_2 son subgrupos normales nilpotentes de G con $G = N_1N_2$, entonces G es nilpotente.

DEMOSTRACIÓN. (1) Se demostró que $F(G) \trianglelefteq G$ y además es un grupo nilpotente. Es decir,

$$F(G) \leq \langle N \mid N \trianglelefteq G \text{ y } N \text{ es nilpotente} \rangle.$$

Sea $N \trianglelefteq G$ nilpotente y sea p un número primo con $p \mid |N|$. Entonces existe $P \in \mathrm{Syl}_p(N)$, con $P \trianglelefteq N$. Esto implica que P char N, y dado que $N \trianglelefteq G$, se tiene que $P \trianglelefteq G$. En consecuencia,

$$P \leq O_p(G) \leq F(G).$$

Como N es nilpotente, se verifica que este es el producto directo de todos sus p-subgrupos de Sylow. Por lo tanto, $N \leq F(G)$, y se tiene además que

$$\langle N \mid N \trianglelefteq G \text{ y } N \text{ es nilpotente} \rangle \leq F(G).$$

(2) La normalidad de $\langle N_1, \ldots, N_r \rangle$ es clara. De (1) se sigue que $\langle N_1, \ldots, N_r \rangle \leq F(G)$. Dado que $F(G)$ es nilpotente, del teorema 8.2.5 se tiene que $\langle N_1, \ldots, N_r \rangle$ es nilpotente.

(3) Este es un caso especial de (2). □

10.2.6 Teorema. Sea G un grupo finito. Entonces

(1) $C_G(F(G))F(G)/F(G)$ no contiene ningún subgrupo normal soluble de $G/F(G)$ distinto del trivial.

(2) $\Phi(G) \leq F(G)$.

(3) Si $G \neq 1$ y G es soluble, entonces $\Phi(G) < F(G)$.

(4) $F(G/\Phi(G)) = F(G)/\Phi(G)$ y además es un grupo abeliano.

DEMOSTRACIÓN. (1) Sea $N/F(G)$ un subgrupo normal abeliano de $G/F(G)$ con $N \leq C_G(F(G))F(G)$. Entonces $N = F(G)C$, donde $C = N \cap C_G(F(G))$. Del segundo teorema de isomorfía se tiene que

$$N/C \cong F(G)/(F(G) \cap C).$$

Sea c la clase de nilpotencia de N/C. Entonces, dado que $N \leq C_G(F(G))F(G)$, se verifica que

$$K_{c+1}(N) \leq C \cap N' \leq C \cap F(G) \leq Z(F(G)) \leq Z(N),$$

con lo cual podemos afirmar que $K_{c+2}(N) = 1$. Es decir, N es nilpotente y, consecuentemente, $N \leq F(G)$. Hemos demostrado entonces que $G/F(G)$ no admite subgrupos normales abelianos contenidos en $C_G(F(G))F(G)/F(G)$. Esto implica que no existen subgrupos normales solubles no triviales de $G/F(G)$ contenidos en $C_G(F(G))F(G)/F(G)$.

(2) En el lema 10.1.7 (1) se demostró que $\Phi(G)$ es nilpotente. Dado que $\Phi(G) \trianglelefteq G$, se tiene que $\Phi(G) \leq F(G)$.

(3) Supongamos que $G \neq 1$ y que G es soluble. Entonces $G/\Phi(G)$ es soluble y no trivial. Por lo tanto, admite un subgrupo normal abeliano no trivial, digamos $M/\Phi(G)$. Por ser abeliano, se verifica que $M/\Phi(G)$ es nilpotente, por lo tanto, del lema 10.1.7 (2) se sigue que M es nilpotente. Entonces $M \leq F(G)$ y se tiene que

$$\Phi(G) < M \leq F(G).$$

(4) La nilpotencia de $F(G)$ implica la nilpotencia de $F(G)/\Phi(G)$. Además, es claro que $F(G)/\Phi(G) \trianglelefteq G/\Phi(G)$. Por lo cual,

$$F(G)/\Phi(G) \leq F(G/\Phi(G)).$$

recíprocamente, escribamos $F(G/\Phi(G))$ en la forma $H/\Phi(G)$, con $\Phi(G) \leq H \leq G$. Dado que $H/\Phi(G)$ es nilpotente, se tiene que H es nilpotente y, en consecuencia, $H \leq F(G)$. Entonces

$$F(G/\Phi(G)) = H/\Phi(G) \leq F(G)/\Phi(G).$$

Para concluir la demostración, note que $F(G) \trianglelefteq G$, por lo tanto,

$$\Phi(F(G)) \leq \Phi(G) \leq F(G).$$

Dado que $\Phi(G)$ es nilpotente, del corolario 10.1.9 se sigue que $F(G)/\Phi(F(G))$ es abeliano. Pero el grupo $F(G)/\Phi(G)$ es isomorfo a un factor de $F(G)/\Phi(F(G))$, por ello, también es abeliano. □

10.2.7 Teorema. Sea G finito. Entonces

(1) Si $N \trianglelefteq G$ y N es abeliano, entonces $N \leq Z(F(G))$.

(2) Si $N \trianglelefteq G$, entonces $N \leq C_G(F(G))$.

Demostración. Dado que $N \trianglelefteq G$, tenemos que $N \cap F(G) = 1$ o $N \cap F(G) = N$.

(1) Si N es abeliano, entonces N es nilpotente y se verifica que $N \leq F(G)$. En consecuencia,

$$1 \neq N \cap Z(F(G)) \trianglelefteq G,$$

y la minimalidad de N implica que $N \leq Z(F(G))$.

(2) Si N no es abeliano, entonces $N \cap F(G) = 1$, ya que de lo contrario $N \leq F(G)$ y se tendría que

$$1 < N' < N,$$

con N' char N y $N \trianglelefteq G$. Es decir, $N' \trianglelefteq G$, lo cual es una contradicción. Pero $N \cap F(G) = 1$ implica que

$$[N, F(G)] \leq N \cap F(G) = 1,$$

y así $N \leq C_G(F(G))$. □

10.2.8 Teorema. Sea $N \trianglelefteq G$ con N nilpotente y $M \lessdot G$ con $N \nleq M$. Entonces $N/(M \cap N)$ es un factor principal de G.

Demostración. Dado que $N \nleq M$, se sigue que $M < MN$, y por la maximalidad de M se tiene que $MN = G$, además $M \cap N < N$. Del teorema 8.2.13 (b) se sigue que $M \cap N < N_N(M \cap N)$. Entonces $N_G(M \cap N)$ es un subgrupo de G que contiene tanto a M como elementos de $N \setminus M$. Así, por la maximalidad de M se sigue que $N_G(M \cap N) = G$. Es decir, $M \cap N \trianglelefteq G$.

Si existiese un subgrupo $K \trianglelefteq G$ con $M \cap N < K < N$, entonces se tendría la cadena de subgrupos $M < MK < G$, lo cual contradice la maximalidad de M. Por lo tanto, $N/(M \cap N)$ es un factor principal de G. □

CAPÍTULO 11

ALGUNOS TEOREMAS DE P. HALL

Dado un conjunto de m chicas y n chicos, sabiendo que cada chica conoce un determinado número de chicos, ¿bajo qué condiciones es posible que todas las chicas puedan casarse / emparejarse / citarse simultáneamente con uno de los chicos entre sus conocidos?
(Philip Hall (1904-1982))

En 1928 Philip Hall demostró que si G es un grupo finito soluble y $|G| = mn$, con $\text{mcd}(m, n) = 1$, entonces G admite subgrupos de orden m y n y en 1937 demostró la afirmación recíproca. Esto representó una nueva caracterización de la solubilidad aparentemente lejos de la presentada inicialmente por E. Galois. La prueba que presentamos hace uso del teorema de Schur[1]-Zassenhaus.

Este teorema, con el cual iniciamos la próxima sección, es sin duda, después de los teoremas de Sylow, uno de los resultados centrales de la teoría de grupos. La búsqueda de complementos de subgrupos normales resulta de gran importancia teórica. Similar como en los teoremas de Sylow y las generalizaciones posteriores de P. Hall, este teorema garantiza la existencia y conjugación de complementos, bajo la imposición de una condición aparentemente simple sobre los órdenes de un subgrupo normal y su correspondiente grupo cociente.

[1]Issai Schur (Mogilev, actual Bielorrusia, 1875-Tel Aviv 1941), matemático judío-alemán. Estudió en Berlín, se doctorøen 1901 y convirtió en profesor en 1903. Fue estudiante de Frobenius y trabajó en representaciones de grupo, combinatoria y física teórica. Schur fue profesor de Richard Brauer, B. H. Neumann, Heinz Prüfer y Richard Rado.

11.1 El teorema de Schur-Zassenhaus

Sea G un grupo y $N \trianglelefteq G$ abeliano. Sabemos que G puede descomponerse como la unión disyunta

$$G = \bigcup_{t \in T} tN,$$

donde T es un transversal izquierdo de N en G. Denotemos con $\mathcal{T}$ el conjunto de todos los transversales derechos de N en G y para $T, S \in \mathcal{T}$ definamos

$$S|T := \prod_{\substack{(s,t) \in S \times T \\ Ns = Nt}} st^{-1}. \tag{11.1}$$

Dado que $sN = tN$ si y solo si $st^{-1} \in N$, se sigue que $S \mid T \in N$. Por otro lado, dado que N es abeliano, se sigue que el orden de los factores en la productoria (11.1) es irrelevante.

11.1.1 Definición. Para $T, S \in \mathcal{T}$ definamos la siguiente relación:

$$S \sim T :\Leftrightarrow S|T = 1. \tag{11.2}$$

11.1.2 Lema. La relación $\sim$ en (11.2) define una relación de equivalencia sobre el conjunto $\mathcal{T}$.

Demostración. Sean $R, S, T \in \mathcal{T}$.

(1) Claramente $R|R = 1$.

(2) Se verifica que $(S|T)^{-1} = T|S$. En efecto,

$$(S|T)^{-1} = \Big(\prod_{\substack{(s,t) \in S \times T \\ Ns = Nt}} st^{-1}\Big)^{-1} = \prod_{\substack{(s,t) \in S \times T \\ Ns = Nt}} ts^{-1} = T|S.$$

Por lo tanto, si $S|T = 1$, entonces $T|S = (S|T)^{-1} = 1$ y se tiene la simetría.

(3) Se verifica que $(R|S)(S|T) = (R|T)$. En efecto,

$$(R|S)(S|T) = \Big(\prod_{\substack{(r,s) \in R \times S \\ Nr = Ns}} rs^{-1}\Big)\Big(\prod_{\substack{(s,t) \in S \times T \\ Ns = Nt}} st^{-1}\Big) = R|T.$$

Por lo tanto, si $R|S = 1$ y $S|T = 1$, se tiene que $R|T = 1$ y se tiene la transitividad. □

Notamos con $[T]$ la clase de equivalencia de $T \in \mathcal{T}$.

11.1.3 Observación. Note que la normalidad de N garantiza no distinguir entre transversales izquierdos y derechos. Por otro lado, demostramos que si $T \in \mathcal{T}$ y $g \in G$, entonces $gT \in \mathcal{T}$. En efecto, si $x \in G$, entonces existen $t \in T$ y $n \in N$ tales que

$$x = tn = g(g^{-1}tn) = gt'n',$$

donde $g^{-1}tN = t'N$, con $t' \in T$.

Por otro lado, si $gtN = gt'N$, se verifica entonces que $tN = t'N$ y, en consecuencia, $t = t'$. Esto implica que G puede descomponerse como la unión disyunta

$$G = \bigcup_{t \in T} gtN.$$

11.1.4 Lema. Sea G un grupo y $\mathcal{T}$ como antes. Consideremos $\circ : G \times \mathcal{T} \longrightarrow \mathcal{T}$ definida por:

$$g \circ T := gT.$$

Entonces $\circ$ define una acción de G sobre $\mathcal{T}$.

Demostración. Sean $g, h \in G$ y $T \in \mathcal{T}$. Entonces

(1) $1 \circ T = 1T = T$.

(2) $(gh) \circ T = (gh)T = g(hT) = g \circ (h \circ T)$. □

11.1.5 Lema. Sea G un grupo, $\mathcal{T}$ como antes y definamos $\Omega := \{[T] \mid T \in \mathcal{T}\}$. Consideremos ahora $\circ : G \times \Omega \longrightarrow \Omega$ definida por

$$g \circ [T] := [gT].$$

Entonces $\circ$ define una acción de G sobre Ω.

Demostración. Sean $g, h \in G$ y $T \in \mathcal{T}$. Entonces

(1) $1 \circ [T] = [1T] = [T]$.

(2) $(gh) \circ [T] = [(gh)T] = [g(hT)] = g \circ (h \circ T)$. □

11.1.6 Lema. Sea G un grupo y $N \trianglelefteq G$ abeliano. Si $g \in G$, $n \in N$ y $T, S \in \mathcal{T}$, entonces

(1) $gS|gT = g(S|T)g^{-1}$.

(2) $[S] = [T] \Leftrightarrow [gS] = [gT]$.

(3) $(nS)|T = n^{|G:N|}(S|T)$. □

Demostración. (1) Usando (11.1) tenemos

$$gS|gT = \prod_{\substack{(s,t)\in S\times T\\ Ngs=Ngt}} (gs)(gt)^{-1} = \prod_{\substack{(s,t)\in S\times T\\ Ngs=Ngt}} g(st)^{-1}g^{-1} = g(S|T)g^{-1}.$$

(2) De $S|T = 1$ se sigue inmediatamente que $gS|gT = 1$, con lo cual se tiene la afirmación.

(3) Nuevamente de (11.1) se tiene que

$$(nS)|T = \prod_{\substack{(ns,t)\in nS\times T\\ Nns=Nt}} nst^{-1} = n^{|G:N|} \prod_{\substack{(s,t)\in S\times T\\ Ns=Nt}} st^{-1} = n^{|G:N|}(S|T). \qquad \square$$

11.1.7 Lema. Sea G un grupo, $N \trianglelefteq G$ abeliano y $\mathrm{mcd}(|N|, |G : N|) = 1$. Entonces la función $\alpha : N \longrightarrow N$ definida por

$$\alpha(n) = n^{|G:N|}$$

define un automorfismo de N.

Demostración. Dado que N es abeliano, se sigue inmediatamente que α es un homomorfismo. De $\mathrm{mcd}(|N|, |G : N|) = 1$ se sigue que existen $a, b \in \mathbb{Z}$ tales que $a|N| + b|G : N| = 1$. En consecuencia, se tiene que

$$n = n^{a|N|+b|G:N|} = n^{b|G:N|}. \tag{11.3}$$

Por lo tanto,

$$n \in \ker(\alpha) \Leftrightarrow n^{|G:N|} = 1 \Leftrightarrow n = 1.$$

Esto demuestra que α es inyectiva y, por lo tanto, un automorfismo. □

11.1.8 Lema. Sea G un grupo, $N \trianglelefteq G$ abeliano, $\mathrm{mcd}(|N|, |G : N|) = 1$ y Ω como antes. Entonces N actúa transitivamente sobre Ω.

Demostración. Sean $S, T \in \mathcal{T}$. Dado que α es sobreyectiva, se sigue que existe $n \in N$ tal que

$$n^{|G:N|} = (S|T)^{-1}.$$

Por lo cual, del lema 11.1.6 (3) se sigue que $(nS)|T = e$. Esto trae como consecuencia que $[nS] = [T]$. Entonces, dados $[S], [T] \in \Omega$, existe $n \in N$ tal que

$$n \circ [S] = [nS] = [T],$$

con lo cual se tiene la afirmación. □

11.1.9 Teorema. Sea G un grupo, $N \trianglelefteq G$ abeliano y $\mathrm{mcd}(|N|, |G:N|) = 1$. Entonces N admite un complemento en G y dos complementos cualesquiera de N en G son conjugados en G.

Demostración. El argumento de Frattini I (teorema 6.1.23) afirma que si G es un grupo, $N \trianglelefteq G$ y Ω un G-conjunto, y si Ω es un N-conjunto transitivo, entonces para todo $[T] \in \Omega$ se verifica que

$$G = G_{[T]}N,$$

donde $G_{[T]}$ es el estabilizador de $[T]$ en G. Esto es,

$$\begin{aligned} G_{[T]} &= \{g \in G \mid g \circ [T] = [T]\} \\ &= \{g \in G \mid [gT] = [T]\} \\ &= \{g \in G \mid gT|T = 1\}. \end{aligned}$$

Sea $n \in N$. Si $(nT)|T = 1$, y dado que $T|T = 1$, se sigue que

$$1 = (nT)|T = n^{|G:N|}(T|T) = n^{|G:N|}.$$

En consecuencia, de (11.3) se sigue que $n = 1$. Esto demuestra que el estabilizador en N de cualquier elemento de Ω es trivial. Por lo tanto, $G_{[T]}$ es un complemento de N en G.

Sea H un complemento de N en G. Entonces para todo $h \in H$ se verifica que $hH = H$, y por lo tanto,

$$(hH)|H = H|H = \prod_{\substack{(x,y)\in H\times H \\ Nx=Ny}} xy^{-1} = 1,$$

ya que por ser H un complemento de N para todo $x, y \in H$ de $Nx = Ny$ se sigue que $x = y$. Esto implica que $H = G_{[H]}$.

Finalmente, dado que N y G actúan transitivamente sobre Ω, se tiene la conjugación de estabilizadores y, por lo tanto, la conjugación de los complementos. (Ver teorema 6.1.13 (4)) $\square$

Consideramos ahora el caso general.

11.1.10 Teorema. (Schur-Zassenhaus) Sea G un grupo, $N \trianglelefteq G$ y $\mathrm{mcd}(|N|, |G:N|) = 1$. Entonces

(1) N admite un complemento en G.

(2) Si N o G/N es soluble, entonces dos complementos cualesquiera de N en G son conjugados en G.

Demostración. (1) Sea G un contraejemplo minimal. Demostramos que N es nilpotente y abeliano.

Sea $P \in \mathrm{Syl}_p(N)$. Del Argumento de Frattini II se sigue que $G = NN_G(P)$. Si $N_G(P) < G$, entonces $|N \cap N_G(P)| < |G|$, y de la minimalidad de G se tendría que $N \cap N_G(P)$ admite un complemento, digamos H, en $N_G(P)$, y además por el segundo teorema de isomorfía

$$|H| = |N_G(P)/(N_G(P) \cap N)| = |N_G(P)N/N)| = |G/N|,$$

con lo que se tendría que H es un complemento de N en G, lo cual no es posible. Esto trae como consecuencia que $N_G(P) = G$. Del teorema 8.2.10 se sigue que N es nilpotente.

Por otro lado, si $N' \neq 1$, entonces, dado que $|G/N'| < |G|$, de la minimalidad de G se tendría que N/N' admite un complemento, digamos M/N', en G/N', y además por el tercer teorema de isomorfía

$$|M/N'| = |G/N'/N/N'| = |G/N|.$$

Dado que N es nilpotente, se tiene que $N' < N$. Por lo cual,

$$|M| = |M/N'||N'| = |G/N||N'| < |G/N||N| < |G|.$$

En consecuencia, existe un complemento de N' en M cuyo orden es $|G/N|$, lo cual es una contradicción. Por lo tanto, $N' = 1$, y así N es abeliano.

Usando el teorema 11.1.9 se tiene la contradicción final.

(2) Sea G un contraejemplo minimal.

Supongamos inicialmente que N es soluble. Entonces $N' < N$. Si $N' = 1$, se tiene entonces que N es abeliano y con el teorema 11.1.9 se obtiene una contradicción.

Supongamos entonces que $N' \neq 1$ y procedamos por inducción sobre $|G|$. Sean H_1, H_2 dos complementos de N en G. Dado que

$$|H_iN'/N'| = |H_i/(H_i \cap N')| = |H_i| = |G/N| = |G/N'/N/N'|,$$

se tiene que cada H_iN'/N' es un complemento de N/N' en G/N' y, en consecuencia, estos son conjugados en G/N'. Es decir, existe $g \in G$ tal que

$$H_1N' = (H_2N')^g = H_2^gN'.$$

Entonces H_1 y H_2^g son complementos de N' en H_1N', y dado que $H_1N' < H_1N = G$, se sigue por la hipótesis de inducción que estos son conjugados en H_1N'. Por lo tanto, existe $h \in G$

$$H_1 = (H_2^g)^h = H_2^{hg},$$

lo cual es una contradicción.

Supongamos ahora que G/N es soluble. Sea $M/N \cdot \trianglelefteq\ G/N$. De la identidad de Dedekind se sigue que

$$M = M \cap H_i N = N(M \cap H_i),$$

con $(M \cap H_i) \trianglelefteq H_i$.

Si $M < G$, entonces los subgrupos $M \cap H_i$ son complementos de N en M, y por la hipótesis de inducción se sigue que estos son conjugados en M. En consecuencia, existe $m \in M$ tal que

$$H_1 \cap M = (H_2 \cap M)^m = H_2^m \cap M.$$

Reemplazando H_2 por $H_1^{m^{-1}}$, si fuese necesario, podemos asumir entonces que $H_2 \cap M = H_1 \cap M$. Si definimos $K := H_1 \cap M$, entonces se tiene que $K \trianglelefteq H_i$ para $i = 1, 2$.

Dado que

$$N_G(K) = N_G(K) \cap H_i N = H_i(N_G(K) \cap N)$$

y

$$(N_G(K) \cap N)K \cap H_i = (N_G(K) \cap N \cap H_i)K = K,$$

se tiene que cada H_i/K es un complemento de $(N_G(K) \cap N)K/K$ en $N_G(K)/K$.

Note que

$$\begin{aligned}(N_G(K)/K)/(N_G(K) \cap N)K/K &\cong N_G(K)/(N_G(K) \cap N)K \\ &\cong N_G(K)/(N_G(K) \cap KN) \\ &= N_G(K)N/KN \\ &\cong (N_G(K)N/N)/(KN/N),\end{aligned}$$

el cual es soluble y, en consecuencia, dado que $|N_G(K)/K| < |G|$, por la hipótesis de inducción los H_i/K son conjugados en $N_G(K)/K$ y se tendría que los H_i son conjugados en G, lo cual es una contradicción.

Solo resta considerar el caso $M = G$. Si esta es la situación, entonces G/N es un grupo soluble y simple. Por lo tanto, un grupo cíclico de orden p para algún número primo p. Dado que $p \nmid |N|$, los complementos de N son precisamente los p-subgrupos de Sylow de G, los cuales son conjugados en G y se tiene la contradicción final. □

11.1.11 Observación. La condición N o G/N soluble en el teorema de Schur - Zassenhaus es irrelevante, ya que de $\text{mcd}(|N|, |G : N|) = 1$ se sigue que el orden de alguno de los dos grupos es impar y por el teorema de Feit-Thompson, soluble.

11.2 Los π-subgrupos de Hall

Notaros con $\mathbb{P}$ el conjunto de todos los número primos y si $\pi \subseteq \mathbb{P}$, entonces usamos π' para denotar el conjunto $\mathbb{P} \setminus \pi$. Es decir, su complemento con respecto el conjunto $\mathbb{P}$. En particular, si π consta de un solo elemento, digamos $\pi = \{p\}$, entonces escribimos p' en lugar de $\{p\}'$. Si G un grupo finito, entonces notamos con $\sigma(G)$ el conjunto de todos los divisores primos de $|G|$.

11.2.1 Definición. Sea G un grupo finito y π un conjunto de números primos.

(1) Un número natural n se denomina un π-`número` si todo divisor primo de n pertenece al conjunto π.

(2) Si $\sigma(G) \subseteq \pi$, entonces G se llama un π-`grupo`. Es decir, si $|G|$ es un π-número.

11.2.2 Ejemplo. Los grupos $\mathrm{Sym}(3)$ y $\mathrm{Sym}(4)$ son $\{2,3\}$-grupos, mientras que $\mathrm{Sym}(5)$ no lo es.

11.2.3 Definición. Sea G un grupo finito, π y σ conjuntos de números primos.

(1) Se define el subgrupo $O_\pi(G)$ de G de la siguiente manera:

$$O_\pi(G) := \langle N \mid N \trianglelefteq G \text{ y } N \text{ es } \pi\text{-grupo} \rangle.$$

(2) De manera dual se define el subgrupo $O^\pi(G)$ de G así:

$$O^\pi(G) := \bigcap \{N \mid N \trianglelefteq G \text{ y } G/N \text{ es } \pi\text{-grupo}\}.$$

11.2.4 Ejemplos. (1) $O_{\{2\}}(\mathrm{Sym}(3)) = \{(1)\}$.

(2) $O_{\{3\}}(\mathrm{Sym}(3)) = \mathrm{Alt}(3) = \{(1), (123), (132)\}$.

Si G es un grupo finito y $N \trianglelefteq G$, el cual es π-grupo, entonces decimos simplemente que N es un π-subgrupo normal de G.

11.2.5 Lema. Sea G un grupo finito y π un conjunto de números primos.

(1) Si G es un π-grupo, entonces todo subgrupo y todo grupo cociente de G también es un π-grupo.

(2) $O_\pi(G)$ char G.

(3) $O_\pi(G)$ es el subgrupo normal más grande de G, que es π-grupo.

Demostración. (1) Sean $U \leq G$ y $N \trianglelefteq G$. Dado que $|U|$ y $|G/N|$ son divisores de $|G|$, se tiene la afirmación.

(2) Sea $\alpha \in \mathrm{Aut}(G)$. Si $N \trianglelefteq G$ es un π-grupo, entonces $\alpha(N) \trianglelefteq G$ y $\alpha(N)$ es un π-grupo. Por lo tanto, $\alpha(O_\pi(G)) \subseteq O_\pi(G)$.

(3) Sean N y M dos π-subgrupos normales de G. Entonces $NM \trianglelefteq G$, y además

$$|NM| = \frac{|N||M|}{|N \cap M|} = |N||M/(N \cap M)|,$$

el cual por (1) es el producto de dos π-números. Por lo cual, $O_\pi(G)$ es el π-subgrupo normal más grande de G. $\square$

En el siguiente teorema presentamos una caracterización los subgrupos $O_\pi(G)$ y $O^{p'}(G)$.

11.2.6 Teorema. Sea G un grupo finito, p un número primo y π un conjunto de números primos.

(1) Si $N \trianglelefteq\trianglelefteq\ G$ y N es un π-grupo, entonces $N \leq O_\pi(G)$. En consecuencia,

$$O_\pi(G) = \langle N \mid N \trianglelefteq\trianglelefteq\ G \ \text{ y } \ N \text{ es } \pi\text{-grupo} \rangle.$$

(2) $O^{p'}(G) = \langle P \mid P \in \mathrm{Syl}_p(G) \rangle = P[P, G]$ para algún $P \in \mathrm{Syl}_p(G)$.

Demostración. (1) Supongamos que $N \trianglelefteq\trianglelefteq\ G$. Es decir, existe una cadena de subgrupos de G de la forma

$$N = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_r = G.$$

Demostramos por inducción matemática sobre r que $N \leq O_\pi(G)$.

Si $r = 1$, entonces $N \trianglelefteq G$, y dado que N es un π-grupo, se sigue que $N \leq O_\pi(G)$.

Sea $r > 1$ y supongamos que está demostrado que $N \leq O_\pi(N_{r-1})$.

De $O_\pi(N_{r-1})$ char N_{r-1} y $N_{r-1} \trianglelefteq G$ se sigue que $O_\pi(N_{r-1}) \trianglelefteq G$. En consecuencia, $O_\pi(N_{r-1}) \leq O_\pi(G)$ y se tiene que $N \leq O_\pi(G)$.

(2) Sean $N := O^{p'}(G)$ y $K := \langle P \mid P \in \mathrm{Syl}_p(G) \rangle$. Si $P \in \mathrm{Syl}_p(G)$, entonces del teorema 6.2.15 se sigue que $PN/N \in \mathrm{Syl}_p(G/N)$. Consecuentemente, $P \leq N$ y, así, $K \leq N$.

Recíprocamente, dado que $\mathrm{Syl}_p(G)$ forma una clase de conjugación, se sigue que $K \trianglelefteq G$. Además $|G:K|$ divide a $|G:P|$, el cual pertenece a p'. Por lo tanto, G/K es un p'-grupo y, en consecuencia, $N \leq K$.

Finalmente, la afirmación $K = P[P,G]$ para algún $P \in \mathrm{Syl}_p(G)$ se sigue del teorema 7.1.9. □

11.2.7 Definición. Sea G un grupo finito, $H \leq G$ y π un conjunto de números primos. H se denomina un π-`subgrupo de Hall` de G si $|H|$ es un π-número y $|G:H|$ es un π'-número. Es claro que H es un π-subgrupo de Hall de G si y solo si $\mathrm{mcd}(|H|,|G:H|) = 1$.

11.2.8 Ejemplo. Sea $G = \mathrm{Alt}(4)$ el grupo alternante de grado 4 y sean

$$V_4 = \{(1),(12)(34),(13)(24),(14)(23)\} \quad \text{y} \quad \pi = \{2,5\}.$$

Tenemos que $|V_4| = 4$ y $|G:V_4| = 3$, por lo tanto, $\mathrm{mcd}(|G:V_4|,|V_4|) = 1$, así se tiene que V_4 es un π-subgrupo de Hall de G.

El conjunto (posiblemente vacío) de todos los π-subgrupos de Hall de G lo notamos con $\mathrm{Hall}_\pi(G)$. Note que si G admite un π-subgrupos de Hall, digamos H, entonces $|H|$ es el más grande π-número que divide a $|G|$. Si en particular $\pi = \{p\}$, entonces $\mathrm{Hall}_\pi(G) = \mathrm{Syl}_p(G)$.

11.2.9 Lema. Sea G un grupo finito, $H \leq G$ y $\pi \subseteq \mathbb{P}$.

(1) $\mathrm{Hall}_\pi(G) = \mathrm{Hall}_{\pi\cap\sigma(G)}(G)$. En consecuencia, 1 es un π-subgrupo de Hall de G si y solo si $\pi \cap \sigma(G) = \varnothing$.

(2) Si H es un π-subgrupo de G, entonces HN/N es un π-subgrupo de G/N.

Demostración. (1) Se sigue inmediatamente de la definición 11.2.7.

(2) Del segundo teorema de isomorfía se sigue que $HN/N \cong H/(H\cap N)$. Por lo cual,

$$|HN/N| = |H/(H\cap N)| = |H : H\cap N|,$$

con lo cual se tiene que cualquier divisor primo de $|HN/N|$ es un divisor de $|H|$ y se tiene la afirmación. □

11.2.10 Lema. Sea G un grupo finito, $\pi \subseteq \mathbb{P}$ y $H \in \mathrm{Hall}_\pi(G)$.

(1) Si $K \leq G$ con $|K| = |H|$, entonces $K \in \mathrm{Hall}_\pi(G)$.

(2) $H^g \in \mathrm{Hall}_\pi(G)$ para todo $g \in G$.

(3) Si $H \leq L \leq G$, entonces $H \in \mathrm{Hall}_\pi(L)$.

Demostración. (1) Dado que $|K| = |H|$, se tiene que $|K|$ es un π-número. Por otro lado,

$$|G : K| = \frac{|G|}{|K|} = \frac{|G|}{|H|} = |G : H|,$$

el cual es un π'-número.

(2) Claramente, $H^g \leq G$ para todo $g \in G$. Además $|H^g| = |H|$, por lo tanto, la afirmación se sigue de (1).

(3) Es suficiente demostrar que $|L : H|$ es un π'-número. Note que

$$|G : H| = |G : L|\ |L : H|.$$

Por lo tanto, todo divisor primo de $|L : H|$ lo es de $|G : H|$, y este es un π'-número. En consecuencia, se tiene la afirmación. □

11.2.11 Lema. Sea G un grupo finito, $\pi \subseteq \mathbb{P}$, $H \in \mathrm{Hall}_\pi(G)$, y $M, N \trianglelefteq G$.

(1) $H \cap N \in \mathrm{Hall}_\pi(H)$.

(2) $HN/N \in \mathrm{Hall}_\pi(G/N)$.

(3) $(H \cap N)(H \cap M) = H \cap MN \in \mathrm{Hall}_\pi(MN)$.

Demostración. (1) Claramente $|H \cap N|$ es un π-número. Por otro lado, note que

$$|N : H \cap N| = \frac{|N|}{|H \cap N|} = \frac{|N||H|}{|H \cap N||H|} = \frac{|HN|}{|H|} = |HN : H|.$$

Dado que $|HN : H|$ divide a $|G : H|$, se tiene que $|N : H \cap N|$ es un π'-número.

(2) Del lema 11.2.9 (2) se sigue que HN/N es un π-grupo. Además

$$|G/N : HN/N| = \frac{|G/N|}{|HN/N|} = \frac{|G|}{|HN|} = |G : HN|.$$

Dado que $|G : HN|$ divide a $|G : H|$, se tiene que $|G/N : HN/N|$ es un π'-número.

(3) Se deja como ejercicio. □

El siguiente resultado se conoce en la literatura como el teorema fundamental de P. Hall. Este garantiza, en el contexto soluble, la existencia, conjugación y dominancia de los π-subgrupos de Hall.

11.2.12 Teorema. (P. Hall, 1928) Sea G un grupo finito soluble y $\pi \subseteq \mathbb{P}$. Entonces

(1) $\mathrm{Hall}_\pi(G) \neq \varnothing$.

(2) Todos los π-subgrupos de Hall de G son conjugados en G. Es decir, Si $H_1, H_2 \in \mathrm{Hall}_\pi(G)$, entonces existe $g \in G$ tal que $H_1^g = H_2$.

(3) Si $H \in \mathrm{Hall}_\pi(G)$ y U es un π-subgrupo de G, entonces $U \leq H^g$ para algún $g \in G$.

Demostración. Procedemos en cada caso por inducción matemática sobre $|G|$. Si $|G| = 1$, entonces las afirmaciones se cumplen trivialmente. Supongamos entonces que $|G| > 1$ y sea N un subgrupo normal minimal de G. Entonces N es un p-grupo para algún número primo p.

(1) Por hipótesis de inducción se tiene que G/N tiene un π-subgrupo de Hall, digamos H/N. Si $p \in \pi$, entonces H es enseguida un π-subgrupo de Hall de G.

Si $p \notin \pi$, entonces por el teorema de Schur - Zassenhaus N tiene un complemento, digamos U, en H. Dado que $|U| = |H/N|$ y

$$\begin{aligned} |G : U| &= |G : H||H : U| \\ &= |G : H||U|, \end{aligned}$$

se sigue que $U \in \mathrm{Hall}_\pi(G)$.

(2) Sean $H_1, H_2 \in \mathrm{Hall}_\pi(G)$. Del lema 11.2.11 (2) se sigue que $H_iN/N \in \mathrm{Hall}_\pi(G/N)$ para $i = 1, 2$. Entonces por la hipótesis de inducción se sigue que

$$H_1N = H_2^gN$$

para algún $g \in G$. Si $p \in \pi$, entonces se tiene que

$$H_1 = H_1N = H_2^gN = H_2^g,$$

como se deseaba.

Si $p \notin \pi$, entonces por el teorema de Schur - Zassenhaus H_1 y H_2^g son complementos de N en H_1N y, por lo tanto, dado que N es abeliano, se tiene que H_1 es conjugado con H_2^g, con lo cual se tiene la afirmación.

(3) Sea U un π-subgrupo de G. Se demostró que todo π-subgrupo de Hall de G/N tiene la forma HN/N para algún $H \in \mathrm{Hall}_\pi(G)$. Entonces por la hipótesis de inducción se sigue que

$$UN/N \leq HN/N,$$

y si $p \in \pi$, entonces concluimos que $U \leq HN = H$.

Si $p \notin \pi$, entonces

$$U \cap N = H \cap N = 1,$$

y si definimos $V := H \cap UN$, tenemos que

$$VN = HN \cap UN = UN.$$

Por lo tanto, U y V son π-subgrupos de Hall de UN y de (2) se sigue que $U = V^x$ para algún $x \in UN$. En consecuencia, $U \subseteq H^x \in \mathrm{Hall}_\pi(G)$. □

11.2.13 Notas. (1) La existencia de π-subgrupos de Hall no puede garantizarse en el contexto general de los grupos finitos. Por ejemplo, si consideramos el grupo $G = \mathrm{Alt}(5)$, se verifica que G no es soluble, $|G| = 2^2 \cdot 3 \cdot 5$, G admite un subgrupo de orden 12 y $\mathrm{mcd}(12, 5) = 1$. Pero también se verifica que G no admite subbgrupos de orden 15 o 20 y sin embargo $\mathrm{mcd}(15, 4) = 1 = \mathrm{mcd}(20, 3)$.

(2) Sea G un grupo finito soluble y supongamos que la factorización en primos distintos de $|G|$ está dada por $|G| = p_1^{a_1} \cdots p_n^{q_n}$. Tanto los teoremas de Sylow como el teorema de Hall garantizan la existencia de un subgrupo de G con orden $p_j^{a_j}$ para todo $j \in \{1, \ldots, n\}$.

El teorema de Hall garantiza además la existencia de subgrupos de Hall con orden

$$p_{j_1}^{a_{j_1}} \cdots p_{j_k}^{a_{j_k}}$$

para $J = \{j_1, \ldots, j_k\} \subseteq \{1, \ldots, n\}$.

El caso más importante se tiene cuando $J = \{1, \ldots, j-1, j+1, \ldots, n\}$ para algún $j \in \{1, \ldots, n\}$. El correspondiente subgrupo se denomina un p_j-`complemento` de G y tiene orden $|G|/p_j^{a_j}$.

Una consecuencia inmediata del teorema de Hall es que todo grupo finito soluble admite p-complemento para todo número primo p con $p \mid |G|$. El recíproco de esta afirmación es válido, ver [6].

Por ejemplo, un grupo finito de orden 105 es soluble por tener orden el producto de tres números primos distintos. Entonces este tiene 3-complementos, es decir, un subgrupo de orden 35, un 5-complemento de orden 21 y un 7-complemento de orden 15.

11.3 Ejercicios

1. Sea G un grupo finito. Demuestre que

   (a) $F(G) = \langle N \mid N \trianglelefteq\trianglelefteq\ G,\ N \text{ es nilpotente}\rangle$.

   (b) Si $N_1, \ldots, N_r$ son subgrupos de G subnormales y nilpotentes, entonces $\langle N_1, \ldots, N_r\rangle$ es también un subgrupo subnormal de G y además nilpotente.

   (c) Si N_1 y N_2 son subgrupos normales nilpotentes de G con $G = N_1N_2$, entonces G es nilpotente.

2. Sea G un grupo no necesariamente finito. Decimos que G satisface la propiedad `max` si todo subconjunto no vacío de subgrupos de G admite un elemento maximal.

   Demuestre que la propiedad `max` es equivalente a

   Todo subgrupo de G es finitamente generado.

3. Sea G un grupo finito soluble. Demuestre que $C_G(F(G)) \leq F(G)$.

4. Sea G un grupo finito, π y σ conjuntos de números primos.

   (a) Se define el subgrupo $O_{\pi,\sigma}(G)$ de G como sigue:

   $$O_{\pi,\sigma}(G)/O_\pi(G) = O_\sigma(G/O_\pi(G)).$$

   (b) De manera dual se define el subgrupo $O^{\pi,\sigma}(G)$ de G como sigue:

   $$O^{\pi,\sigma}(G) = O^\sigma(O^\pi(G)).$$

   Demuestre que

   (a) $O^\pi(G)$ es un subgrupo característico de G.

   (b) $O^\pi(G)$ es el subgrupo normal más pequeño de G con la propiedad que su cociente $G/O^\pi(G)$ es un π-grupo.

   (c) $O_{\pi,\sigma}(G)$ es un subgrupo característico de G.

LISTA DE SÍMBOLOS

$\mathbb{N}$	conjunto de los números naturales
$\mathbb{Z}$	conjunto de los números enteros
$\mathbb{Q}$	conjunto de los números racionales
$\mathbb{R}$	conjunto de los números reales
$\mathbb{C}$	conjunto de los números complejos
$\mathbb{P}$	conjunto de los números primos
π'	complemento de $\pi \subseteq \mathbb{P}$ en $\mathbb{P}$
p'	complemento de $p \in \mathbb{P}$ en $\mathbb{P}$
$\mathbb{F}_p$	cuerpo finito con p elementos
$\mathbb{Z}_n$	grupo de las clases residuales módulo n
$K^\times$	grupo multiplicativo de un cuerpo
$G, H, \ldots$	grupos
$\|G\|$	número de elementos del grupo G
$H \leq G$	H es un subgrupo de G
$H < G$	H es subgrupo propio de G
$N \trianglelefteq G$	N es subgrupo normal de G
$N \triangleleft G$	$N \trianglelefteq G$ y $N \neq G$
$M \lessdot G$	M es un subgrupo maximal de G
$H \trianglelefteq\trianglelefteq G$	H es subgrupo subnormal de G
H char G	H es subgrupo característico de G
$\|G : H\|$	índice del subgrupo H en G
$\langle X \rangle$	subgrupo generado por X
$\langle X_i \mid i \in I \rangle$	subgrupo generado por $\bigcup_{i \in I} X_i$
X^g	$g^{-1}Xg$ para un grupo G, $g \in G, X \subseteq G$

1	elemento neutro de un grupo o el grupo de orden 1
g^h	conjugado de g con h
$[g,h]$	conmutador de g con h
$[U,V]$	subgrupo conmutador de U con V
V_4	4-grupo de Klein
$\mathrm{Sym}(X)$	grupo de permutaciones de un conjunto X
$\mathrm{Sym}(n)$	grupo simétrico de grado n
$\mathrm{Alt}(n)$	grupo alternante de grado n
D_{2n}	grupo dihedral de grado n
$\mathbb{Q}_8$	grupo de los cuaterniones
$\cong$	relación de isomorfía entre grupos
G/N	el grupo cociente de G módulo N
$N_G(X)$	normalizador de X en G
$C_G(X)$	centralizador de X en G
$Z(G)$	centro de G
$\mathrm{Core}_G(H)$	el core de H en G
G'	subgrupo conmutador o derivado de G
$\Phi(G)$	subgrupo de Frattini de G
$F(G)$	subgrupo de Fitting de G
$\mathrm{Aut}(G)$	grupo de automorfismos de G
$\mathrm{Syl}_p(G)$	conjunto de los p-subgrupos de Sylow de G
$\mathrm{Hall}_\pi(G)$	conjunto de los π-subgrupos de Hall de G
$G \rtimes_\alpha H$	producto semidirecto de G con H vía α
$X \wr_\alpha G$	producto orlado de X con G respecto a α
$K_i(G)$	i-ésimo elemento de la cadena central descendente
$Z_i(G)$	i-ésimo elemento de la cadena central ascendente
$U(n)$	Grupo de las n-ésimas raíces complejas de la unidad
$\sigma(G)$	conjunto de todos los divisores primos de $\lvert G\rvert$
$O_\pi(G)$	$\langle N \mid N \trianglelefteq G$ y N es π-grupo$\rangle$
$O^\pi(G)$	$\bigcap\{N \mid N \trianglelefteq G$ y G/N es π-grupo$\}$

ÍNDICE DE NOMBRES

Burnside, W.	188, 195
Cayley, A.	124
Cauchy, L. A.	128
Feit, W.	188
Fitting, H.	197
Frattini, G.	125, 131, 189, 192
Hall, Ph.	210, 212
Hölder, O.	182
Jordan, C.	182
Klein, F.	4, 49
Kronecker, L.	1
Lagrange, J. L.	23
Schreier, O	179
Schur, I.	201, 202
Sylow, L.	126
Thompson, J.	188
Weber, H.	1
Wielandt, H.	126, 193
Witt, E.	169
Zassenhaus, H. J.	202

ALFABETO GRIEGO

A	α	alpha
B	β	beta
Γ	γ	gamma
Δ	δ	delta
E	ϵ	epsilon
Z	ζ	zeta
E	η	eta
Θ	θ	theta
I	ι	iota
K	κ	kappa
Λ	λ	lambda
M	μ	my
N	ν	ny
Ξ	ξ	xi
O	o	omicron
Π	π	pi
P	ρ	rho
Σ	σ	sigma
T	τ	tau
Υ	υ	upsilon
Φ	ϕ	phi
X	χ	ji
Ψ	ψ	psi
Ω	ω	omega

BIBLIOGRAFÍA

[1] J. F. Caicedo. *Teoría de Grupos*, Universidad Nacional de Colombia, 2004.

[2] J. Dixon. *Problems in Group Theory*, Courier Dover Publications, 1973.

[3] K. Doerk and T. Hawkes. *Finite soluble groups*, Berlín - New York : Walter de Gruyter, 1992.

[4] D. Gorenstein. *Finite groups*, New York : Chelsea, 1980.

[5] M. Hall Jr. *Teoría de los grupos,* Trillas, 1979.

[6] P. Hall. *A characteristic property of soluble groups,* J. London Math. Soc. 12, 1937.

[7] I. N. Herstein. *Álgebra moderna*, Bogotá: Trillas, 1967.

[8] H. Hungerford. *Algebra*, GTM 73, Springer - Verlag, 2003.

[9] B. Huppert. *Endliche Gruppen I*, Springer - Verlag, 1969.

[10] H. Kurzweil and B. Stellmacher. *The theory of finite groups: an introduction*, Springer - Verlag, 2004.

[11] J. Rotman. *An introduction to the Treory of Groups*, 4th edition, GTM 148, New York: Springer - Verlag, 1999.

[12] D. J. S. Robinson. *A Course in the Theory of Groups*, 2th edition, GTM 80, New York: Springer - Verlag, 1996.

[13] H. E. Rose. *A Course on finite groups*, Universitext - Springer, 2009.

[14] J. S. Rose. *A Course on Group Theory*, Dover Publications, 1994.

[15] W. R. Scott. *Group Theory*, Courier Dover Publications, 2010.

[16] M. Suzuki. *Group Theory I*, Springer - Verlag, 1977.

[17] G. Smith and O. Tabachnikova. *Topics in group theory*, Springer - Verlag, 2000.

ÍNDICE ALFABÉTICO

2-ciclo, 78
G-conjuntos, 131
π-grupo, 222
π-número, 222
π-subgrupos de Hall, 221, 222, 224
k-ciclo, 78
p-subgrupo de Sylow, 143
p-subgrupos de Sylow, 140
Órbita, 134
3-ciclos, 84
4-grupo de Klein, 18, 41, 56

Acción de un grupo sobre un conjunto, 131
Acción transitiva de un grupo sobre un conjunto, 135
Argumento de Fratini I, 139
Argumento de Frattini II, 145
Automorfismo, 52
    exterior, 63
    interior, 54
Automorfismos exteriores, 63
Automorfismos interiores, 54

Centralizador, 65
Centralizador de un elemento en un grupo, 136
Clase de conjugación, 64
Clase de nilpotencia de un grupo, 178
Clases laterales derechas, 35
Clases laterales izquierdas, 35
Clasificación de grupos, 40
Clausura normal, 160
Complemento de un subgrupo, 152
Conmutator, 160
Core
    propiedades, 137
Core de un subgrupo, 137

Derivados de orden superior, 166
Descomposición en clases laterales, 36

Ecuación de las clases, 139
El subgrupo de Frattini, 203
Elementos conjugados, 48
Elementos de torsión, 89
Endomorfismo, 52
Epimorfismo, 52
Estabilizador, 134
Estabilizador y la órbita, 135

Factor directo, 110
Factor principal, 196

Grupo, 16
    centro de, 65
    cociente, 50
    factor, 50
    lineal especial de grado n, 17
    lineal general de grado n, 17

simétrico, 18
abeliano, 16
alternante, 77, 83
cíclico, 25, 91
centro de un, 62
conmutativo, 16
finitamente generado, 25
finito, 16
generado por un conjunto, 25
libre de torsión, 89
orden de un, 16
simétrico de grado n, 77
simple, 49
sistema de generadores, 25
Grupo abeliano
elemental, 153
tipo de un, 153
Grupo alternante, 77
Grupo cíclico, 89
clasificación, 98
generadores de un, 98
grupo de automorfismos, 100
subgrupos de un, 95
Grupo cociente, 50
Grupo de las unidades complejas, 24
Grupo de los cuaterniones, 32
Grupo de permutaciones, 18
Grupo de Prüfer, 90
Grupo de simetrías de un triángulo, 27
Grupo de simetrías del cuadrado, 30
Grupo dihédrico o diedral de grado n, 27
Grupo factor, 50
Grupo lineal especial de grado n, 17, 22, 53
Grupo lineal general de grado n, 17
Grupo simétrico de grado n, 18, 77
Grupos abelianos finitamente generados, 150
Grupos abelianos finitos, 150
Grupos nilpotentes finitos, 178
Grupos solubles finitos, 168

Homomorfismo, 52
automorfismo, 52
endomorfismo, 52
epimorfismo, 52
imagen de un, 52
isomorfismo, 52
kernel de un, 52
monomorfismo, 52
nucleo de un, 52

Identidad de Dedekind, 34
Identidad de Hall-Witt, 183
Inverso de un elemento, 18
Involución, 89
Inyección canónica, 119
Isomorfismo, 52

Lema de los tres subgrupos, 183
Lema de Poincaré, 39
Lema de Zassenhaus, 189, 190
Lema del punto fijo, 139
Lemma de Frattini, 206
Leyes de cancelación, 20

Monomorfismo, 52

Número de clases, 64
Nilpotencia y solubilidad, 182
Normalizador, 65

Orden de un elemento, 89
Orden de un elemento en un grupo, 21

Permutación
signo de una, 80
Permutaciones
disyuntas, 78
impares, 83
notación de ciclos, 78
pares, 83
Potencias, 20
Potencias enteras, 20
Potencias naturales, 20
Producto cartesiano, 106, 115, 119

Producto complejo, 32, 34
Producto de Frobenius, 32
Producto directo, 115
    externo, 115
    externo no restringido, 115, 119
Producto directo externo - caso finito, 106
Producto directo externo - caso infinito, 114
Producto directo interno, 110
Producto orlado, 130
Producto semidirecto, 124
    interno, 124
Proyección canónica, 116

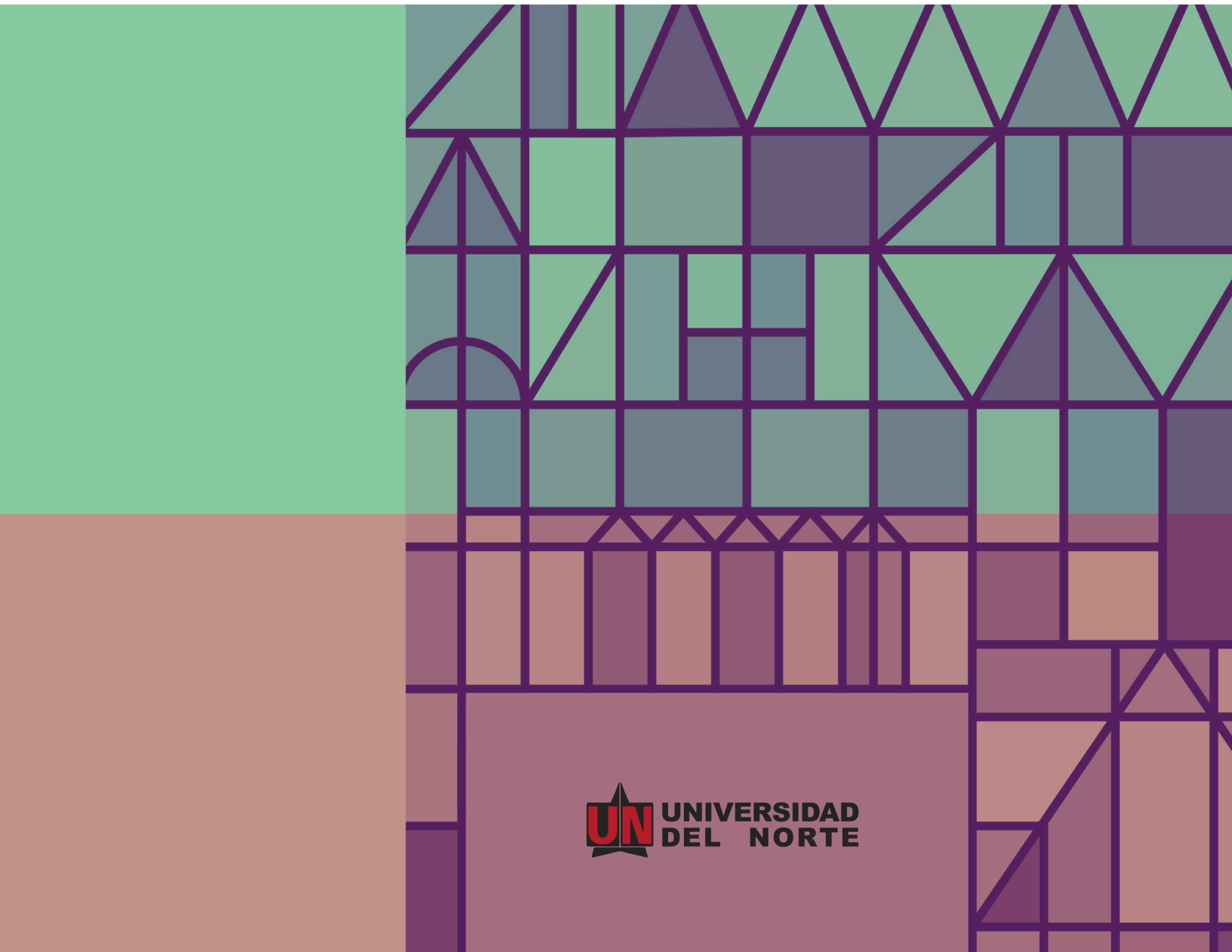
Raíces complejas de la unidad, 25
Representaciones por permutaciones, 131

Serie
    factor principal, 196
Serie central, 173
Serie central ascendente, 173, 175
Serie central descendente, 173, 175
Serie de composición, 196
Serie de subgrupos, 190
    longitud, 190
Serie normal de subgrupos, 190
serie principal, 196
Serie subnormal de subgrupos, 190
Signo, 80
Sistema de generadores de un grupo, 25
Sistema de representantes, 36
Subgrupo, 22
    índice de un, 36
    normal, 48
    caacterístico, 67
    completamente invariante, 67
    maximal, 22
    propio, 22
Subgrupo conmutator, 160
Subgrupo de Fitting, 210, 211
Subgrupo derivado, 160
Subgrupo normal, 48
    propio, 48
Subgrupos
    finitos, 23
Subgrupos de $\mathbb{Z}$, 23
Subgrupos normales minimales, 199
Subgrupos triviales, 22
Suma directa, 119
    externa, 119
    externa restringida, 119
Sumando directo, 110

Teorema de Cauchy, 142
Teorema de Cayley, 138
Teorema de correspondencia, 59
Teorema de isomorfía I, 56
Teorema de isomorfía II, 57
Teorema de isomorfía III, 58
Teorema de Jordan - Hölder, 189
Teorema de la base de Burnside, 209
Teorema de Lagrange, 35
Teorema de Schreier, 193
Teorema de Schur - Zassenhaus, 215, 221
Teorema de Wielandt, 206
Teorema fundamental de la aritmética, 197
Teorema fundamental de los grupos abelianos, 153
Teoremas de Hall, 225
Teoremas de Sylow, 144
    aplicaciones, 147
Transposición, 78
Transversal derecho, 36
Transversal izquierdo, 36

Valor absoluto, 56

Esta obra se editó en Barranquilla por
Editorial Universidad del Norte, en marzo de 2022.
Se compuso en LaTex con - Computer Modern (CM).

En este texto se presentan resultados básicos sobre la teoría de grupos, haciendo especial énfasis en los grupos finitos. Se demuestran teoremas estructurales como el de Jordan-Hoelder, los de Sylow y las extensiones de estos últimos en el universo de los grupos solubles, los teoremas de Hall.

El objetivo central es brindar una herramienta formal y elegante de los fundamentos del álgebra a estudiantes de ciencias, especialmente los de matemáticas a nivel de pregrado y posgrado.